CHRISTCHURCH
HARPENDEN

Data Protection Policy

"Data Protection Legislation" or "Legislation"	means the Data Protection Act 1998, the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), the General Data Protection Regulation (GDPR), any laws in the UK enacting the GDPR or preserving its effect in whole or part following the departure of the UK from the European Union and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, together with, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office.

Data Protection Legislation is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully and that where necessary the privacy of individuals is respected. During the course of the activities of ChristChurch Harpenden ("the Church"), the Church will collect, store and process personal data about our members, people who attend our services and activities, employees, suppliers and other third parties and we recognise that the correct and lawful treatment of this data will help maintain confidence in the Church. This policy sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

The Data Protection Compliance Manager is responsible for ensuring compliance with the Legislation and with this policy. The post is held by

the Operations & Communications Manager who can be contacted at office@christchurchharpenden.org.uk

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 Compliance Manager.

Reviewed by: Fraser Keir & Sarah Vickers
Accepted by the Trustees: 4 March 2019

Processing personal data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action.

Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.

Personal data is data relating to a living individual. It includes employee data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered. Personal data can be factual (for example a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Examples of personal data are employee details, including employment records, names and addresses and other information relating to individuals, including supplier details, any third-party data and any recorded information including any recorded telephone conversations, emails or CCTV images.

Employees and others **(including volunteers and trustees)** who process data on behalf of the Church (referred to in this policy as 'Employees') should assume that whatever they do with personal data will be considered to constitute processing.

Employees should only process data:

- If they have consent to do so; or
- If it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship; for example, processing the payroll; or
- the processing is **necessary for legitimate interests** pursued by ChristChurch Harpenden, unless these are overridden by the interests, rights and freedoms of the data subject.

If none of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

Compliance with the Legislation

Employees who process data on our behalf have a responsibility for processing personal data in accordance with the Legislation. This includes the data protection principles in the Legislation. These state that personal data must:

- be obtained and used fairly, lawfully and transparently
- be obtained for specified, explicit and legitimate purposes and used only for those purposes
- be adequate, relevant and limited to the minimum necessary for those purposes

- be accurate and kept up to date (every reasonable endeavour should be used to ensure that personal data that is not accurate is corrected or erased without delay)
- be processed in a manner that ensures its security (*see Information Security policy at Appendix 1).*
- not be kept for any longer than required for those purposes *see Retention policy at Appendix 2).*

We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice) unless there is a legal exemption from doing so. We will keep records of any information shared with a third party including a record of any exemption which has been applied.

Employees should follow the Data Breach Procedure *(at Appendix 3)* if they think they have accidentally breached any provision of this Data Protection Policy.

Sensitive data

We will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards can be put in place. Sensitive data means data consisting of information relating to an individual's

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health, and genetic information
- Sexual life
- Criminal offences

Sensitive data may be processed in the course of our legitimate activities, but may not be passed to any third party without the express consent of the data subject.

Monitoring the use of personal data

We are committed to ensuring that this data protection policy is put into practice and that appropriate working practices are being followed. To this end the following steps will be taken:

- any Employees who deal with personal data are expected to be aware of data protection issues and to work towards continuous improvement of the proper processing of personal data;

- Employees who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored;
- All Employees must consider whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure inaccurate, excessive or out of date data is disposed of in accordance with this policy;
- Employees must follow the procedures contained in the Data Breach Policy (*at Appendix 3)* should they become aware of any breach of this policy;
- Employees will keep clear records of our processing activities and of the decisions we make concerning personal data (including reasons for the decisions) to show how we comply with the Legislation;
- Spot checks may be carried out;
- An annual report on the level of compliance with or variance from good data protection practices will be produced by the Communications & Operations Manager
- Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences;
- We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

Handling personal data and data security

This will be managed in accordance with our Information Security Policy *(see Appendix 1)*.

The rights of individuals

The Legislation gives individuals certain rights to know what data is held about them and what it is used for. If personal data is collected directly from an individual, we will inform them in writing of their rights by providing them with a 'Privacy Notice' at the time the personal data is collected or as soon as possible afterwards.

In principle everyone has the right to see copies of all personal data held about them. There is also a right to have any inaccuracies in data corrected or erased. Data subjects may also have a right of portability in respect of their personal data, and a right to be forgotten. Data subjects also have the right to prevent the processing of their data for direct marketing purposes.

Any request for access to data under the Legislation should be made to the Communications & Operations Manager in writing at office@christchurchharpenden.org.uk

n accordance with the Legislation we will ensure that written requests for access to personal data are complied with within **20 days** of receipt of a valid request (where

permitted under the Legislation, we may take a further 20 days to respond but we will inform the individual of why this is necessary).

When a written data subject access request is received the data subject will be given a description of a) the personal data, b) the purposes for which it is being processed, c) those people and organisations to whom the data may be disclosed, d) be provided with a copy of the information in an intelligible form.

Changes to this policy

We reserve the right to change this policy at any time, including as needed to comply with changes in law. Where appropriate we will notify data subjects of those changes by mail or email.

This policy adopted at the Trustees meeting held on .....

To be reviewed in 12 months

Appendices attached to this policy:-

APPENDIX 1 - Information Security Policy

APPENDIX 2 - Records Retention Policy

APPENDIX 3 - Data Breach Policy

APPENDIX 4 - Complaints process

APPENDIX 5 - CCH Guidance on keeping personal data safe and secure

Information Security Policy Appendix 1

Information security involves preserving confidentiality, preventing unauthorised access and disclosure, maintaining the integrity of information, safeguarding accuracy and ensuring access to information when required by authorised users.

In addition to complying with this policy, all users must comply with the Data Protection Legislation and the Data Protection Policy.

'Church data' means any personal data processed by or on behalf of ChristChurch Harpenden.

Information security is the responsibility of every member of staff, trustee, office holder, church member and volunteer using Church data on, but not limited to, the Church information systems. This policy is the responsibility of the Communications & Operations Manager who will undertake supervision of the policy.

Our IT systems may only be used for authorised purposes. We will monitor the use of our systems from time to time. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. In particular:

- All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed.
- Manual records relating to church members or staff will be kept secure in locked cabinets. Access to such records will be restricted.
- Access to systems on which information is stored must be password protected with strong passwords and these should be changed at once if there is a risk they have been compromised. Passwords must not be disclosed to others.
- We will ensure that staff, church leaders, trustees, members and volunteers who handle personal data are adequately trained and monitored to ensure data is being kept secure.
- We will ensure that only those who need access will have access to data.
- We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out in the CCH Data Protection Policy), e.g. password protection for documents and encryption.
- Where personal data needs to be deleted or destroyed adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files. Particular care should be taken over the destruction of manual sensitive data (written records) including shredding or disposing via specialist contractors (who will be treated as data processors -see below).
- We will ensure that any data processor engaged to process data on our behalf (e.g. for payroll) will act under a written contract and will give appropriate undertakings as to the security of data.
- Appropriate software security measures will be implemented and kept up to date.
- We will ensure that if information has to be transported or transferred, this is done safely using encrypted devices or services.
- Where personal devices are used to store or process personal data, they must be subject to appropriate security.

All breaches of this policy must be reported to the Communications & Operations Manger on office@christchurchharpenden.org.uk

See also ‘CCH Guidance on keeping personal data safe and secure’.(Appendix 5)

This policy will be regularly reviewed and audited.

This policy adopted at the Trustees meeting held on .....

To be reviewed in 12 months

Records Retention Policy Appendix 2

Storage of Data and Records Statement

1. All data and records will be stored in accordance with the security requirements of the Data Protection Legislation and in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

2. Data and records which are active should be stored in the most appropriate place for their purpose commensurate with security requirements.

3. Data and records which are no longer active, due to their age or subject, should be stored in the most appropriate place for their purpose or destroyed.

4. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded.

5. Any data file or record which contains personal data of any form can be considered as confidential in nature.

6. Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Legislation, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose". All staff, trustees, volunteers and members of the Church are required to have regard to the Guidelines for Retention of Personal Data table attached hereto and to the CCH 'Guidance on keeping personal data safe and secure' (Appendix 5).

7. Any data that is to be disposed must be safely disposed of for example by shredding. Any group which does not have access to a shredder should pass material to the Communications & Operations Manager who can be contacted on office @christchurchharpenden.org.uk, who will undertake secure shredding.

8. Special care must be given to disposing of data stored in electronic media. Guidance will be given by the Communications & Operations Manager to any group which has stored personal data relating to its members on for example personal computers which are to be disposed of And further guidance can be found in the 'CCH Guidance on keeping personal data safe and secure' (Appendix 5).

This policy adopted at the Trustees meeting held on .....

To be reviewed in 12 months

Guidelines for Retention of Personal Data

(This is not an exhaustive list)

If you have any queries regarding retaining or disposing of data please contact the Operations & Communications Manager on office@christchurchharpenden.org.uk

Types of Data	Suggested Retention Period
Human Resources Records including training records and notes of disciplinary and grievance hearings.	• 7 years from the end of employment
Application forms / interview notes	• Maximum of one year from the date of the interviews for those not subsequently employed. If employed, retain in personnel file.
Information relating to children *NB. the following article is helpful* http://safeinchurch.org.uk/record-retention	
Consent forms for attendance at a **specific** children's / youth activity	• Until the specific activity / trip is over **unless** there has been a serious accident or incident – then keep 100 years.
Records of concern about a child or young person Records about a disclosure made by a child or young person	• 100 years
Records of allegations against a member of staff or volunteer	• 100 years
Child /Youth Information Sheets	• Until the child ceases to attend the group
Group Attendance records	• Digital information to be kept for 100 years. Paper copies to be securely destroyed three years after the child ceased to attend the group. • There is a need to retain this information in the event of future allegations of historic abuse.

DBS Records (digital and paper)	• If the individual is not renewing their DBS the both paper and digital record are to be destroyed / deleted immediately.
Church member information	• Check for accuracy once a year • Record that adult was a member – permanent • Secure destruction of personal data other than name and fact of membership – three years after cease to be a member •
Church group member information	• Check for accuracy once a year • Record that adult was a member of group – permanent • Secure destruction of personal data other than name and fact of membership – three years after cease to be a member of the group •
Statutory Financial information, including correspondence with tax office	• 7 years after the end of the financial year to which the records relate
Wages and salary records	• 7 years from the tax year in which generated
Accident books, and records and reports of accidents	• (for Adults) 3 years after the date of the last entry • (for children) three years after the child attains 18 years
Health records	• 6 months from date of leaving employment • (Management of Health and Safety at Work Regulations)
Health records where reason for termination of employment is connected with health, including stress related illness	• 3 years from date of leaving employment • (Limitation period for personal injury) claims)
Student records, including academic achievements, and conduct	• At least 6 years from the date the student leaves in case of litigation for negligence
Pastoral Meeting notes (adults & children)	• 3 years after last contact
Photos	• Keep for no longer that three years then securely destroy / delete

Data Breach Policy Appendix 3

Introduction

ChristChurch Harpenden ("we") hold and process personal data which needs to be protected. Every care is taken to protect the data we hold. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties.

Purpose

This policy sets out the procedure to be followed to ensure a consistent and effective approach throughout the Church.

Scope

The policy relates to all personal data held by ChristChurch Harpenden, regardless of format. It applies to *anyone* who handles this personal data, including those working on behalf of the Church both in a paid and in a voluntary capacity. The objective of the policy is to contain any breaches, to minimise the risks associated with the breach and to consider what action is necessary to secure personal data and prevent any further breach.

Types of breach

An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects.

An incident includes but is not restricted to:

- Loss or theft of personal data or the equipment on which the data is stored e.g. laptop, memory stick, smartphone, or paper record
- theft or failure of equipment on which personal data is stored
- Unauthorised use of or access to personal data
- Attempts to gain unauthorised access to personal data
- Unauthorised disclosure of personal data
- Website defacement
- Hacking attack

Reporting an incident

Any person using personal data on behalf of ChristChurch Harpenden is responsible for reporting data breach incidents immediately to the Operations & Communications Manager on office@christchurchharpenden.org.uk or in his or her absence the Chair of Trustees, also on office@christchurchharpenden.org.uk or 01582 769165

The report should contain the following details:

- Date and time of discovery of breach
- Details of person who discovered the breach
- The nature of the personal data involved
- How many individuals' data is affected

Containment and recovery

The Communications & Operations Manager will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Consideration will be given as to whether the police should be informed. Advice from appropriate experts will be sought if necessary. A suitable course of action will be taken to ensure a resolution to the breach.

Investigation and risk assessment

An investigation will be carried out without delay and where possible within 2 working days of the breach being discovered. The Communications & Operations Manager will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to occur.

The investigation will take into account the following:

- The type of data involved and its sensitivity
- The protections in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to illegal or inappropriate use
- Who the data subjects are, how many are involved, and the potential effects on them
- Any wider consequences

Notification

The Communications & Operations Manager will decide, with appropriate advice, who needs to be notified of the breach. Every incident will be assessed on a case by case basis. The Information Commissioner will be notified, if at all possible within 24 hours of the data breach, if a large number of people are affected or the consequences for the data subjects are very serious. Guidance on when and how to notify the ICO is available on their website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Where appropriate, we will notify the data subjects whose personal data has been affected by the incident; such a notification may include a description of how and when the breach occurred, and the nature of the data involved, and specific and clear advice on what they can do to protect themselves and what has already been done to mitigate the risks.

The Communications & Operations Manager will keep a record of all actions taken in respect of the breach.

Evaluation and response

Once the incident is contained, the Communications & Operations Manager will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring.

This review will be discussed with the Chair of Trustees and reported at the next Trustees meeting.

This policy adopted at the Trustees meeting held on .....

To be reviewed in 12 months

Data Protection Complaints Process Appendix 4

ChristChurch Harpenden ("we") take your privacy concerns seriously. If you have any concerns about the way your information is being handled, please contact the Operations & Communications Manager without delay on office@christchurchharpenden.or.uk or 07784 962059

We will carefully investigate and review all complaints and take appropriate action in accordance with Data Protection Legislation. We will keep you informed of the progress of our investigation and the outcome. If you are not satisfied with the outcome, you may wish to contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Any complaint must be in writing and must clearly outline the nature of the issue, who was involved, what the impact was and what you would expect to be an appropriate remedy. We cannot accept anonymous complaints. You cannot complain on behalf of another adult unless you have their permission in writing.

Any complaint must be sent to the Operations & Communications Manager who will arrange for an investigation as follows:

1. A record will be made of the details of the complaint.
2. Consideration will be given as to whether the circumstances amount to a breach of Data Protection Legislation and action taken in accordance with the Data Breach Procedure.
3. The complainant will be kept informed of the progress of the complaint and of the outcome of the investigation. The outcome will be communicated in writing within 30 days of the complaint being received.
4. At the conclusion of the investigation the Operations & Communications Manager will reflect on the circumstances and recommend to Christchurch Harpenden Trustees any improvements to systems or procedures.

If you are not satisfied by the outcome of the complaint you may lodge in writing a appeal within 7 days of receiving the outcome of your complaint. This appeal will be hear by persons not involved in the original complaint.

This policy adopted at the Trustees meeting held on .....

To be reviewed in 12 months

Guidance on keeping personal data safe and secure **Appendix 5**

Introduction to data protection and GDPR

1. The Information Commissioners Office (ICO) provides advice and guidance on the use of data in the UK. This falls into the realm of the General Data Protection Regulation (GDPR) 2018. On the ICO website you can find all you need to know about how your data should be controlled and processed. CCH is registered with the ICO and we encourage you to look at the very accessible information on www.ico.org.uk for more information. In the meantime, this information sheet will help orientate you to the obligations of the General Data Protection Regulation (GDPR). You should also review the policies which can be obtained from the Operations & Communications Manager on office@christchurchharpenden.org.uk

General Data Protection Regulation (GDPR)

There are 10 rights under GDPR.

- Your right to be informed if your personal data is being used. This means CCH must inform you if it is using your personal data.
- Your right to get copies of your data. This means you have the right to find out if an organisation is using or storing your personal data.
- Your right to get your data corrected. This means you can challenge the accuracy of personal data held about you by an organisation.
- Your right to get your data deleted. This means you can ask CCH to delete personal data that it holds about you.
- Your right to limit how organisations use your data. This means you can limit the way an organisation uses your personal data.
- Your right to data portability. This means you have the right to get your personal data from an organisation in a way that is accessible.
- The right to object to the use of your data. This means you have the right to object to the processing or use of your personal data in some circumstances.
- Your rights relating to decisions being made about you without human involvement. This means decisions are made about you when your personal data is processed automatically.
- Your right to access information from a public body. This means you can make a request for information from a public body.
- Your right to raise a concern. This means you can talk to CCH if you're concerned about how they are using your data.

Personal data

2. This means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This can include your email address as it identifies you, your Twitter handle or facebook name. Your image is also a way to identify you and that is why we ask for permission when taking a video or a photo during CCH activities.
3. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
4. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data such as the CCH Church Directory or membership records.

Sensitive personal data

5. The GDPR refers to sensitive personal data as “special categories of personal data”. This data relates to race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; sexual orientation. ChristChurch Harpenden does not routinely gather (or need) all these categories of sensitive personal data.
6. The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
7. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Stay secure when working remotely

8. As a church and a charity we have both a moral and legal responsibility to look after the flock under our care and one way we can serve our church well is by looking after their data. The following information is guidance in pursuit of the above and to help support the implementation the General Data Protection Regulation (GDPR) 2018. If a data breach occurs you have a responsibility to inform the Church Communications & Operations Manager so that the ICO and data subject can be made aware of the breach.
9. There are various ways to access CCH online resources such as iKnowChurch, rotas, email distribution lists, directories, files and systems and services when working at home or in your office. Almost all of our volunteering activity is undertaken outside of the Vaughan Road building and consequently there is an individual responsibility to ensure personal and sensitive information is kept safely and securely. If you have any questions about the guidance contained in here please do say so. The guidance is not mean to

be a list of 'dos' and 'don't's but rather some recommendations to help us look after the data and information under our stewardship.

Take care when using personal devices

10. Take extra care when using portable personal devices such as laptops, smartphones and tablets. Be sure to use passcodes, passwords and security settings, such as encryption and, if need be, remote wiping, to reduce the potential impact of losing information. The following guidance will help you consider how to keep data and information secure.

    - Install up to date virus and malware protection
    - Using your computer with out of date virus protection, or none at all, will leave you open to new threats. Make sure your personal computers and devices have virus and malware protection and that you update them regularly.
    - Be aware when working in public spaces. Just being around other people is enough to put information at risk. Be aware of people or cameras looking over your shoulder when typing in your account details and view information with care.
    - Internet cafés might seem convenient but be wary of accessing sensitive information on any equipment that you do not trust. Keyboard input can be tracked by anybody else accessing the machine, through a process known as keylogging, which allows them to record all of the keys you press on the keyboard. Avoid using Internet cafés to access sensitive or valuable data.
    - Even a few moments spent away from your working area is enough for somebody to have seen something they were not supposed to. You should always lock your computer when you leave it and keep any written documents out of view or in a locked container.
    - Never leave your device unattended and never share your password. Its good practise to have a password that is not linked to identifiable data. Consider using uppercase and lowercase letters, numbers and symbols when constructing a password. Again you should change your password regularly.

Back up documents regularly

11. Backing up your important documents and information regularly can minimise the effects of stolen data and technical failures. Your computer is not backed up by default so you should consider secondary storage.

12. If you have to copy sensitive information to a device that you own, make sure you are complying with CCH and the Information Commissioners Office. You should always make sure that the information retains a level of security protection and is deleted from the system as soon as it is no longer necessary

for it to be there**.** You should familiarise yourself with the CCH Data Retention Policy.

Cloud storage

13. There are benefits to using cloud storage providers, including the ability to easily share and sync documents across multiple devices and potentially with external collaborators. However, many consumer web-based cloud storage providers do not always encrypt (protect) data adequately. This means data could be accessed, shared or lost and there have been a number of high profile cases of personal data infringements reported in the press due to storing data and photos on cloud platforms.

14. Data stored with cloud service providers is outside of your control, meaning that the company could change their terms and conditions or upgrade their hardware or software without your permission or knowledge. In the past, problems with upgrades have caused data to be exposed on the Internet. Your data may be stored outside the European Union, meaning that is it subject to local not UK law. This could enable third parties in other countries to access your data.

Access to cloud storage data could also be removed at any time and this is also outside of your control. This could result in your account and any related data being deleted. So, if you are storing sensitive or confidential CCH data on one of these platforms, please speak to the CCH Communications & Operations Manager for guidance and support.

15. Microsoft's OneDrive for Business offers high standards for data security and resilience ensuring compliance to the most common data protection frameworks and standards. Microsoft ensures that data is only held in the EU. Your data can only be accessed or viewed by you as the owner of the file, or those you choose to give permissions to for collaboration and not by Microsoft or anyone else. CCH does not endorse the purchase of this product but raises it as an example of how data can be safely and efficiently stored.

Email distribution lists

16. Those sending messages to any mass email list are asked to adhere to the following guidelines.IN data protection terms a 'mass email' is any distribution list with multiple email addresses on it.

    - Make sure the email addresses on your distribution are current and that the recipient could reasonably expect to receive an email from you.

- Do not put the distribution list or list of names in the ‘To’ or ‘CC’ fields. Instead, include them in the ‘BCC’ field. This method ensures the list of recipients will not be displayed when the email is sent out, and prevents recipients accidently sending their reply to the whole list. This process can considerably cut down on unnecessary email traffic.
- Make the subject line clear and concise. This will allow personal filtering by subject easier for recipients. (Research shows that many people choose whether to open an email based on the subject line alone.)
- Do not send mass emails with large attachment as this slows the email network and blocks individual in-boxes. Try to contain the information within the body of the email or in a web link.
- Make the text of the email as clear and unambiguous, ensuring that the text has been thoroughly checked for spelling, punctuation and grammar.
- Keep emails as brief as possible. The more concise the message, the more likely it will have the desired impact and be read by a large number of people.
- Include contact details for those who have questions or require further information.
- If you are regularly sending communications from ChristChurch Harpenden you should use a xxxx.xxxx@christchurchharpenden.org.uk It is common practise to automatically redirect personal emails into a single mailbox.

Removable Media

17. Using removable media such as USB keys, hard drives, memory cards and DVDs have a number of risks associated with them and so, should be carefully considered as an option before use.

18. Removable media can store vast amounts of information but, due to their design and portability, they are very easy to steal or lose. If the device contains sensitive data then it should be protected to prevent misuse.

19. If you find a device or are given data on removable media from an unknown source, do not connect it to your computer. It may contain malware that could infect your machine.

20. Any removable media device that is used to store data should be password-protected and the information stored on it encrypted, to prevent misuse. And, if you must use a USB device, make sure it's not your only copy!

ChristChurch Harpenden **February 2019**

Reviewed by Fraser Keir & Sarah Vickers
Accepted by the Trustees: 4 March 2019

Reviewed by Fraser Keir & Sarah Vickers
Accepted by the Trustees: 4 March 2019