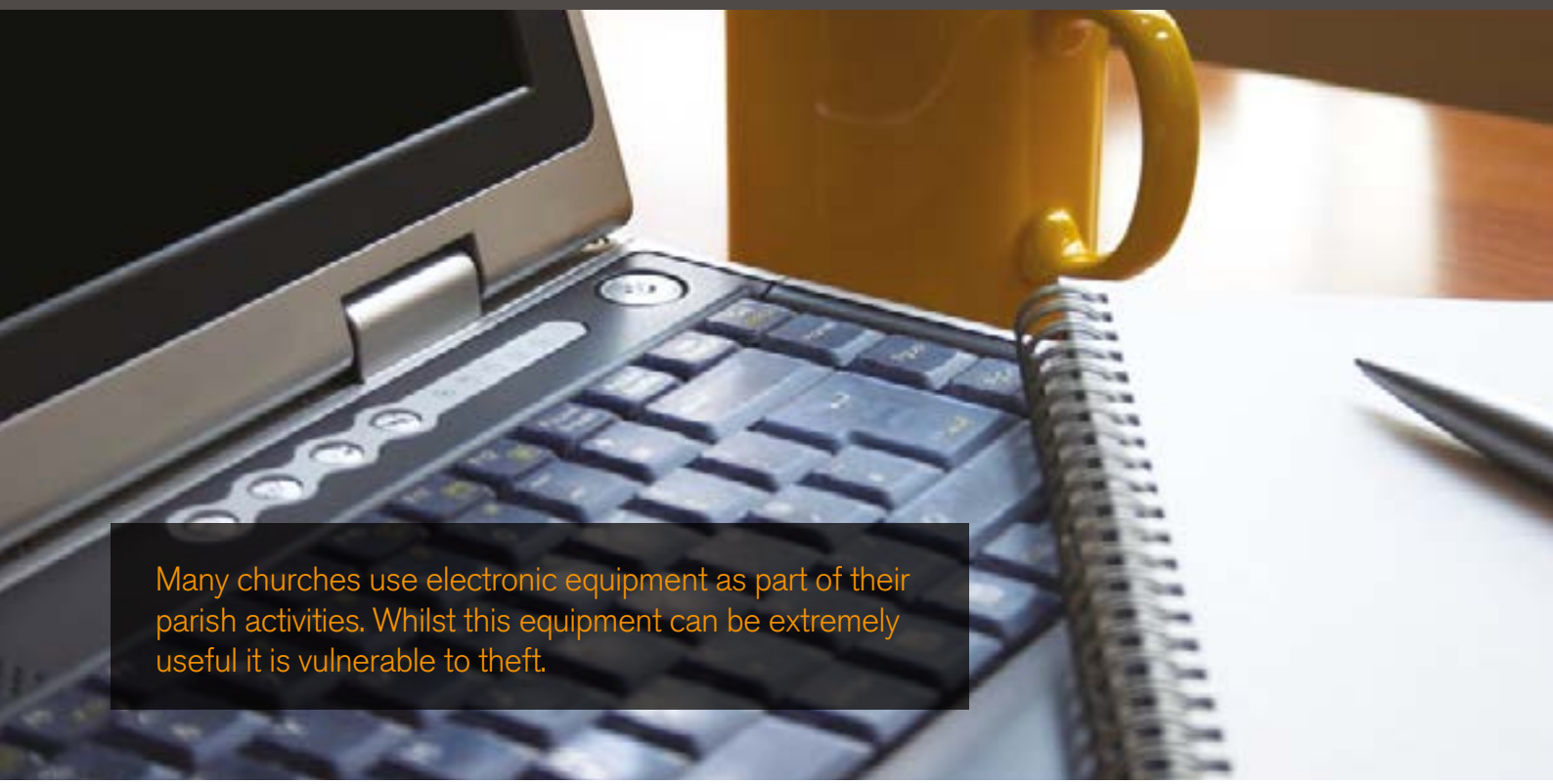
Church security guidance

Protection and use of electronic equipment



Many churches use electronic equipment as part of their parish activities. Whilst this equipment can be extremely useful it is vulnerable to theft.

Physical security for electronic equipment

Many churches use computer equipment of some type. These are generally portable, saleable and therefore very attractive to thieves. Church computers are commonly either kept in the church/parish office, at the parsonage or at the home of another church official. Many churches use portable projectors and sophisticated sound systems. These items, like computers, are most attractive to thieves. The physical security that we would normally recommend would include:

- perimeter doors secured by five lever mortice deadlocks to BS 3621. If the equipment is kept in a vestry in an otherwise open church, the internal vestry door should be similarly protected
- accessible opening windows should be protected by key operated window locks
- if possible, equipment should be sited such that it is not readily visible from the outside
- purchase receipts should be retained or the model and serial numbers recorded which will help the Gardaí and Ecclesiastical in the event of any theft
- electronic equipment should be permanently marked with an identifying name and postcode. Markings should be prominently visible and/or advertised to deter would-be thieves. Leased or rented equipment should not be marked without the prior agreement of the company concerned
- lockdown plates and computer enclosure devices (preferably tested to LPS 1214 category I and II) can be used to secure computer and ancillary equipment to desks/work surfaces
- projectors and sound equipment should be protected by security enclosures. Ecclesiastical can provide further information on suppliers if required.

ecclesiastical

Security of laptops and tablet computers

Due to their highly portable nature, laptops and tablets are even more vulnerable to theft than PCs and the following security measures should be followed:

- under normal circumstances do not leave them unattended even for short periods
- if for some reason a laptop or tablet has to be left unattended then it should be secured in a purpose-built store/ security cabinet or at least out of sight in a locked room
- they should not be put down when in a public area
- the laptop or tablet should be etched with an identifying name and postcode. If the item is leased, then a check should first be made with the leasing company
- they should not be left in offices overnight unless they are locked within purpose-built storage units or, as a minimum, in a locked filing cabinet
- details of the equipment including serial numbers must be recorded in the assets register together with the name of the person to whom it has been issued
- carry cases should not advertise the fact that they contain a computer
- when travelling by car keep the equipment in the boot of the car and keep both boot and doors locked
- be aware of people around you, particularly when loading or unloading the car or in a public place. Avoid using the equipment in a public place
- make sure that back-ups of the information are kept in a secure location and not in the carry case.

Intruder alarm protection for electronic equipment

It is strongly recommended that, in addition to good physical security, an intruder alarm system is installed where computers and other electronic equipment are in use. For more detailed information on intruder alarms see our separate guidance entitled 'Installation of intruder alarms'.

Backup data

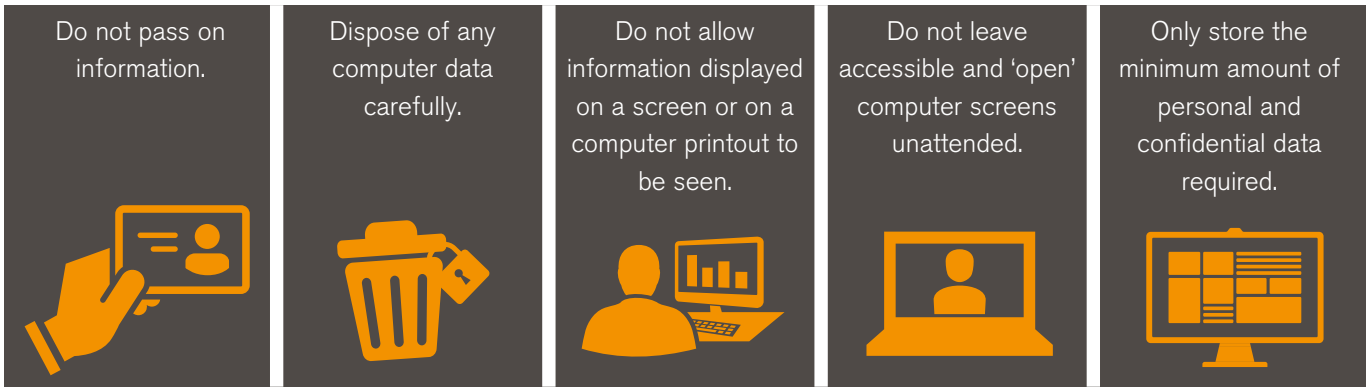
It is advisable to keep backup copies of data at another location. This avoids inconvenience in the case of theft or fire. To comply with the provisions of the General Data Protection Regulation (GDPR) these should be securely protected.

General Data Protection Regulation (GDPR)

GDPR is intended to protect individual's personal data. GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The data held on parish computers would not normally be a target for theft, but data might be stolen with parish equipment. To protect parish data, encryption should be used on all parish computers. In addition to the physical security outlined above, the following points should be considered:



Need to contact us?

For further advice Ecclesiastical customers can call our Risk Management Team on **01 619 0300** (Monday to Friday 9am - 5pm, excluding bank holidays)

ecclesiastical

Ecclesiastical Insurance Office plc is regulated by the Central Bank of Ireland.

Ecclesiastical Insurance Office plc Reg. No. 24869. Registered in England at Benefact House, 2000 Pioneer Avenue, Gloucester Business Park, Brockworth, Gloucester, GL3 4AW, United Kingdom. Registered Branch in Dublin, Ireland. Reg No. 902180. 2nd Floor, Block F2, EastPoint, Dublin 3. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority in the United Kingdom (Firm Reference Number 113848).