Information Security Policy documentation

## Legal requirement

Article 5(1)(f) of the GDPR concerns the ‘integrity and confidentiality’ of personal data. It says that personal data shall be:

'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'

Article 32(1) of GDPR states:

‘This means that we must have appropriate security to prevent the personal data we hold being accidentally or deliberately compromised. We should remember that while information security is sometimes considered as cybersecurity, it also covers other things like physical and organisational security measures.’

‘Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk’

## The checklist

* We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place. In our schedule
* When deciding what measures to implement, we take account of the state of the art and costs of implementation. Yes we do
* We have an information security policy (or equivalent) and take steps to make sure the policy is implemented. In our schedule
* Where necessary, we have additional policies and ensure that controls are in place to enforce them. Not necessary
* We make sure that we regularly review our information security policies and measures and, where necessary, improve them. In our schedule
* We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials. Not appropriate
* We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process. Not appropriate
* We use encryption and/or pseudonymisation where it is appropriate to do so. Yes we do
* We understand the requirements of confidentiality, integrity and availability for the personal data we process. Yes we do
* We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. Backup procedure to be established
* We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. In our schedule
* Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism. Not appropriate
* We ensure that any data processor we use also implements appropriate technical and organisational measures. Not appropriate

### What do our security measures need to protect?

We should ensure that:

* **the data can be accessed, altered, disclosed or deleted only by those we have authorised to do so (and that those people only act within the scope of the authority we give them);**
* the data we hold is accurate and complete in relation to why we are processing it; and
* the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, we should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

What security measures are appropriate will depend on our own circumstances, the processing we are doing, and the risks it presents to our church. An Information Risk Assessment is required. We need to consider the scope of the data and the people who access it.

### What technical measures do we need to consider?

When considering physical security, we should look at factors such as:

* the quality of doors and locks, and the protection of our premises by such means as alarms, security lighting or CCTV;
* how we control access to our premises, and how visitors are supervised;
* how we dispose of any paper and electronic waste; and
* how we keep IT equipment, particularly mobile devices, secure.

When considering cybersecurity, we should look at factors such as:

* system security – the security of our network and information systems, including those which process personal data;
* data security – the security of the data we hold within your systems, eg ensuring appropriate access controls are in place and that data is held securely;
* online security – eg the security of our website and any other online service or application that you use; and
* device security – including policies on Bring-your-own-Device (BYOD) if you offer it.

Whatever we do, we should remember the following:

* our cybersecurity measures need to be appropriate to the size and use of our network and information systems;
* we should take into account the state of technological development, but we are also able to consider the costs of implementation;
* our security must be appropriate to our business practices. For example, if we offer staff the ability to work from home, we need to put measures in place to ensure that this does not compromise your security; and
* our measures must be appropriate to the nature of the personal data we hold and the harm that might result from any compromise.

### Should we use pseudonymisation and encryption?

If we are storing personal data, or transmitting it over the internet, we are recommend by the Information Commissioner’s Office to use encryption and have a suitable policy in place, taking account of the residual risks involved.

### What are ‘confidentiality, integrity, availability’ and ‘resilience’?

Confidentiality, integrity and availability are the three key elements of information security. If any of the three elements is compromised, then there can be serious consequences, both for us as a data controller, and for the individuals whose data we process.

The information security measures you implement should seek to guarantee all three both for the systems themselves and any data they process.

We are also required to have the ability to ensure the ‘resilience’ of our processing systems and services. Resilience refers to:

* whether our systems can continue operating under adverse conditions, such as those that may result from a physical or technical incident; and
* our ability to restore them to an effective state.

This refers to things like business continuity plans, disaster recovery, and cyber resilience.

### What are the requirements for restoring availability and access to personal data?

We must have the ability to restore the availability and access to personal data in the event of a physical or technical incident in a ‘timely manner’.

### Are we required to ensure our security measures are effective?

Yes, the GDPR specifically requires us to have a process for regularly testing, assessing and evaluating the effectiveness of any measures we put in place. What these tests look like, and how regularly we do them, will depend on our own circumstances. However, it’s important to note that the requirement in the GDPR concerns our measures in their entirety, therefore whatever ‘scope’ we choose for this testing should be appropriate to what we are doing, how we are doing it, and the data that we are processing.

Technically, we can undertake this through a number of techniques, such as vulnerability scanning and penetration testing. These are essentially ‘stress tests’ of your network and information systems, which are designed to reveal areas of potential risk and things that we can improve.

**Some industries are required to undertake tests of security measures on a regular basis. The GDPR now makes this an obligation for all organisations**. Importantly, it does not specify the type of testing, nor how regularly we should undertake it. It depends on our church and the personal data we are processing.

We can undertake testing internally or externally. In some cases it is recommended that both take place.

Whatever form of testing we undertake, we should document the results and make sure that we act upon any recommendations, or have a valid reason for not doing so, and implement appropriate safeguards. This is particularly important if our testing reveals potential critical flaws that could result in a personal data breach.