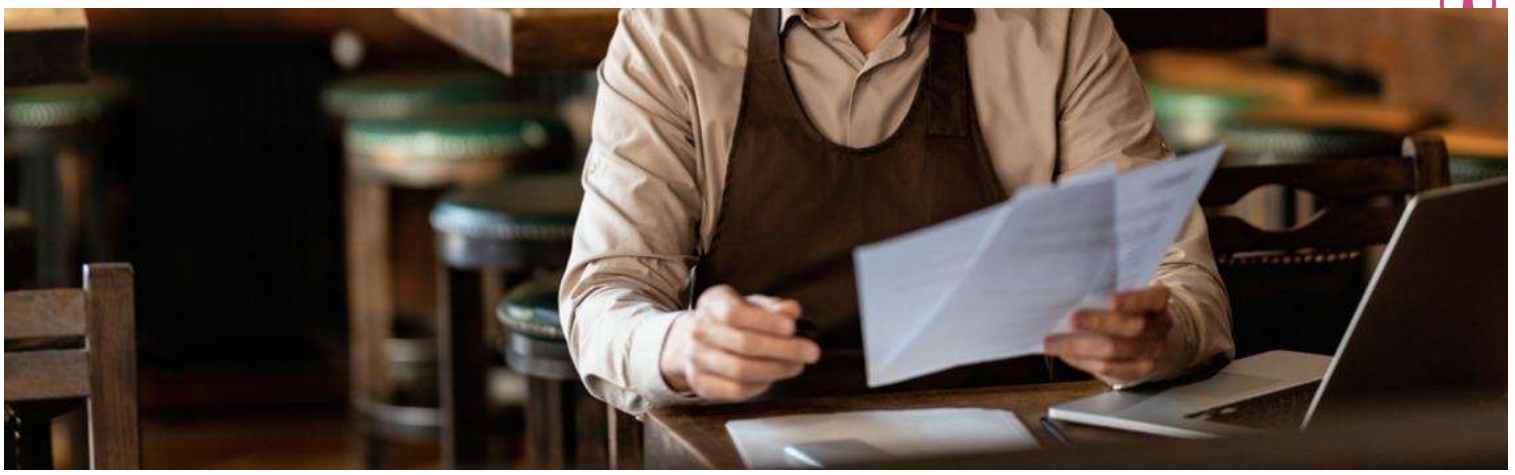
Nine cyber and data security documents your business needs

BLOGS 14 Dec 2021

Protect your data, your business, and your bottom line with these key documents, templates and guides for cyber security and data protection.



Being your own boss means you're responsible for protecting your business against the threat of cyber-attacks and data breaches. With seven million cyber-crimes targeted at small businesses in the UK every year, these incidents can happen to any business, no matter how small. It's vital to put measures in place to safeguard your business.

Protecting company and customer data is also a legal requirement under the Data Protection Act (2018), which incorporates the UK General Data Protection Regulation (UK GDPR). All data or information that relates to an identifiable individual that your business stores or handles

needs to be properly protected, whether it's staff information or a client's personal details.

Failing to adequately protect your business can be costly. According to the **Cyber Security Breaches Survey 2021**, the average cost of a cyber incident for a small business is £8,460, not to mention the potential for fines for non-compliance.

Thankfully, there are measures, policies and processes you can put in place. You'll note that some of these are legally required and others are highly recommended. Experts from **FSB Legal Hub** explain what they're used for and why they're so important.

1. Cyber security policy (Recommended)

A **cyber security policy** provides guidelines for how your online systems and software should be used to minimise risk. It helps everyone in your business to understand the processes you have in place to protect your company, data and assets from cyber criminals or from accidental data loss.

2. UK GDPR data processing agreement (Required)

A data processing agreement is a contract between a data controller and a data processor. For example, your company may be engaging with a third-party who will be processing personal data on behalf of your client. The agreement establishes how the data will be used and why, and it's required to ensure data protection rules are followed.

3. Website privacy notice (Required)

A privacy notice for a website states the purpose of data collection on your website. For example, if you are collecting personal data from your clients, you need to provide a link to your privacy notice. It explains what data you're collecting, why you're collecting it and how it will be used.

4. Data protection policy (Recommended)

This document explains how your business protects personal data and the measures you put in place to comply with data protection laws. It covers areas such as data processing, roles and responsibilities, and contact information.

5. Business password policy (Recommended)

A business password policy is a set of rules that you and your team follow to increase cyber security and reduce the risk of cyber criminals getting access to your systems. The **National Cyber Security Centre** has further guidance on secure password strategies you can implement.

6. Employee exit checklist (Recommended)

An employee leaving your business, whether for pastures new or due to dismissal, can present cyber security issues, for example preventing unauthorised access when someone no longer works for you. Revoking access to your systems and devices is especially important if the employee was handling sensitive or confidential information.

Find out more about **what to do when an employee leaves your business**.

7. Cyber security due diligence questionnaire for third parties (Recommended)

Working with external companies? You should be choosing your suppliers with cyber security and data protection in mind.

If you rely on third parties to process your data, such as your suppliers or services providers, then you're responsible for any personal data that is handled by third parties that contract with you and you should check they have appropriate data protection measures in place.

8. Personal data subject access request response letter (Required)

Under data protection laws, everyone has the right to request a copy of the personal information that a business holds on them. There are strict rules in place for abiding by these requests, which are enforced by the **Information Commissioners Office (ICO)**.

9. Cookie policy (Required)

The data protection rules provide detailed guidance around the requirement and use of cookies on websites. It's important to understand these. Your responsibility includes telling people that you use cookies, explaining what they do and why it's needed, and getting consent to store a cookie on their device.

Download your free documents now

FSB members have access to documents, guides and template policies via FSB Legal Hub, covering a variety of data and cyber security matters to help keep your small business secure and compliant.

Legal compliance is just a click away

With FSB Legal Hub, you'll have legal documents at your fingertips. Search over 1,400 documents, templates, policies and more, on everything from tax to cyber security. Checked by real lawyers, fully compliant and easy to use.

Related resources

ARTICLE Tue, 09 August 2022

How to register a new business

VIDEO Thu, 23 June 2022

Make Your Business an Inclusive Workplace

VIDEO Thu, 23 June 2022

Make your business more accessible

Our mission is to help smaller businesses achieve their ambitions

We offer our members a wide range of vital business services including advice, financial expertise, support and a powerful voice heard in government

Design and build by Pixl8