

Website Security Responsibility Policy

Introduction

This policy applies to customers of Ashford Web Services and outlines the responsibilities related to website security following the development or handover of a WordPress site. Operated by Gary Friend as a Sole Trader, Ashford Web Services provides clients with professional website builds, but maintaining a secure website is a shared responsibility.

This document sets out the customer's role in protecting their website from unauthorised access and explains the terms under which Ashford Web Services may assist with security-related issues.

Customer Responsibility

1. Security Measures

Customers are fully responsible for implementing and maintaining their own website security after launch or handover. Key measures include:

- Using strong, unique passwords for WordPress admin and hosting accounts
- Keeping WordPress core, themes, and plugins updated to the latest versions
- Installing and configuring appropriate security plugins (e.g. firewalls, login protection)
- Regularly reviewing security logs and settings
- Monitoring for suspicious activity or performance issues

2. Backups

Customers are responsible for setting up and maintaining regular website backups. Backups should be created before making any significant changes and stored securely outside of the website's hosting environment. Regular backups are essential for mitigating the risk of permanent data loss in the event of errors, failed updates, or security breaches.

3. Login Confidentiality

Login credentials must not be shared with unauthorised parties. Customers are responsible for securing admin access and maintaining confidentiality. Sharing login information increases the risk of unauthorised access and compromises overall site security.

Developer's Role

1. Support Availability

If a customer suspects a security breach or unauthorised access, I am available to assist with investigation, recovery, and remediation at an hourly rate of £55. This

applies to time spent identifying issues, restoring backups, applying fixes, or strengthening protection.

2. Limitations

While I will make every reasonable effort to support recovery, I cannot guarantee full restoration in all cases. The success of recovery depends on factors such as the nature of the breach, availability of backups, and the hosting environment. Ashford Web Services does not provide continuous security monitoring unless covered under a separate agreement.

Indemnification

Customers agree to indemnify and hold Ashford Web Services harmless from any claims, damages, or losses resulting from unauthorised access, hacking, or poor security practices following project handover. This includes, but is not limited to, data loss, site downtime, and third-party liabilities.

Final Thoughts

This policy is designed to promote responsible website ownership by clearly outlining post-handover responsibilities. By following best practices and maintaining proper backups and security protocols, customers can ensure the ongoing safety and integrity of their website.

Last updated: 29th May 2025