

Byrne Dean Cyber Security Policy

1. Introduction

This document sets out the measures to be taken by all employees of Byrne Dean (the “Company”) and by the Company as a whole in order to protect the Company’s computer systems, devices, infrastructure, computing environment and any and all other relevant equipment (collectively, “IT Systems”) from damage and threats whether internal, external, deliberate or accidental.

2. Anti-Virus Security Measures

- Most IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall and internet security software. All such anti-virus, firewall and internet security software will be kept up to date with the latest software updates and definitions.
- All IT Systems protected by anti-virus software will be subject to a full system scan at least once a week.
- Users shall be permitted to transfer files using cloud storage systems. All files downloaded from any cloud storage system must be scanned for viruses during the download process.
- Any files being sent to third parties outside the Company, whether by email, on physical media or by other means (e.g., FTP or shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate. All email attachments are scanned automatically upon sending.
- Where any virus is detected by a User this must be reported immediately to the IT Department (this rule shall apply even where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Wherever possible a suitable replacement computer or device will be provided to limit disruption to the User.
- Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Company’s disciplinary procedures.

3. Data Protection

All personal data (as defined in The General Data Protection Regulation 2016/679) collected, held and processed by the Company will be collected, held and processed strictly in accordance with the Data Protection Principles of The General Data Protection Regulation 2016/679 and the provisions of the Data Protection Act 2018.

4. Reporting IT Security Breaches

All concerns, questions, suspected breaches or known breaches shall be referred immediately to IT Department.

Upon receiving a question or notification of a breach, the IT Department shall, within 30 minutes, assess the issue including, but not limited to, the level of risk associated therewith, and shall take any and all such steps as the IT Department deems necessary to respond to the issue.

Under no circumstances should a User attempt to resolve an IT security breach on their own without first consulting the IT Department. Users may only attempt to resolve IT security breaches under the instruction of, and with the express permission of, the IT Department.

All IT security breaches, whether remedied by the IT Department or by a User under the IT Department's direction, shall be fully documented.

5. Protection from Cyber-attacks

All Users are responsible for managing cyber risks and therefore must understand and comply with this policy and associated guidance. Users should be aware of:

- what information they are using, how it should be protectively handled and stored
- how to report a suspected breach of information security within the company
- their responsibility for raising any information security concerns with senior management

Senior Managers are responsible for ensuring that all Users are aware of the cyber policy and obligations.

- Public Wi-Fi hotspots should not be used as somebody could access your login details and what you are working on whilst you are connected. 3G/4G/5G networks should be used instead as these have built-in security.
- Only share your email address with people you trust. Be wary of opening emails from contacts that are unknown to you and be suspicious of attachments and links from the emails you receive, especially if it's from contacts you do not know.
- Care should be exercised when accessing internet sites. Untrustworthy sites, especially those that encourage users to download content, can be used to infect devices with malware. Always ensure that websites and links to websites, come from a trustworthy source.

Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in an email or other forms of communication. Attackers will commonly use phishing emails to distribute malicious links or attachments that can perform a variety of functions. Some will extract login credentials or account information from victims.

Typically, a victim receives a message that appears to have been sent by a known contact or organization. The attack is then carried out either through a malicious file attachment, or through links connecting to malicious websites. In either case, the objective is to install malware on the user's device or direct the victim to a fake website. Fake websites are set up to trick victims into divulging personal and financial information, such as passwords, account IDs or credit card details.

If Users think they have been the victim of a phishing attempt or cyber-attack, including inadvertently downloading malware, follow the procedure for reporting in section 9 above. For insurance purposes the Data Protection Officer

(COO) or the Finance Team should also be informed who will report the attack in the appropriate way. All incidents of cyber-attack must be reported using cfc Response (The Finance Team and Operations team have access to this).

6. Implementation of Policy

This Policy shall be deemed effective as of November 2022. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.