Cybersecurity Policy

Last updated Jan 8, 2026

Contents

Cybersecurity Policy 3

Policy brief & purpose 3

Scope 3

Policy elements 3

Confidential data 3

Protect personal and company devices 3

Keep emails safe 4

Manage passwords properly 4

Transfer data securely 5

Additional measures 5

Disciplinary Action 6

Take security seriously 6

Mobile Phone Policy 7

Policy brief & purpose 7

Scope 7

Policy elements 7

How to properly use mobile phones in the workplace 8

Disciplinary Consequences 8

Email Policy 9

Policy brief & purpose 9

Scope 9

Policy elements 9

Inappropriate use of company email 9

Appropriate use of corporate email 10
Personal use 10
Email security 10
Email signature 11
Disciplinary action 11
Internet usage policy 12
Policy brief & purpose 12
Scope 12
Foveal LLP internet usage policy elements 12
What is appropriate employee internet usage? 12
What is inappropriate employee internet usage? 12
Company-issued equipment 13
Email 13
Disciplinary Action 13

Cybersecurity Policy

Policy brief & purpose

Foveal LLP cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise our company's reputation.

For this reason, we have implemented several security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

This policy applies to all Foveal LLP Partners (referred to as Partners hereon), employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our partners and employees instructions on how to avoid security breaches.

Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They must:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive company-issued equipment, we ensure:

- Password management tool setup
- Installation of antivirus/ anti-malware software

They should follow instructions to protect their devices and refer to a if they have any questions.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct partners and employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can refer to a Partner

Manage passwords properly

Foveal LLP ensures Multi factor Authentication to access all company related software, email clients, and files.

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)

- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in person isn't possible, employees should prefer the phone instead of email, and only if they personally recognise the person they are talking to.
- Change their passwords every 90 days.

Transfer data securely

Transferring data introduces a security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we employees must ask a Partner for permission and help.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Our Partners need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Foveal LLP will investigate promptly, resolve the issue and send a companywide alert when necessary.

Our Security Specialists are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to a Partner.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to refrain from using social media for any Foveal LLP-related business, with our internet usage policy.

Foveal LLP has and will:

- Installed firewalls, anti-malware software and access authentication systems.
- Arranged for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Our company will have all physical and digital shields to protect information.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Take security seriously

Everyone, from our customers to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Mobile Phone Policy

Policy brief & purpose

Foveal LLP's **employee mobile phone policy** outlines our guidelines for using mobile phones at work.

We recognise that mobile phones (and smartphones especially) have become an integral part of everyday life. They may be a great asset if used correctly (for productivity apps, calendars, business calls, etc.)

But mobile phones may also cause problems when used imprudently or excessively.

Scope

This policy applies to all our Foveal LLP Partners (referred to as Partners hereon), employees and contractors.

Policy elements

Despite their benefits, personal mobile phones may cause problems in the workplace. Employees who use their mobile phones excessively may:

- Cause security issues from inappropriate use of company-issued equipment or misuse of our company's internet connection.

Our company expects employees to use their mobile phones prudently during working hours.

We won't allow employees to:

- Play games on the mobile phone during working hours.
- Use their phones for any reason while driving a company vehicle.
- Use their mobile phone's camera or microphone to record confidential information.
- Use their phones in areas where mobile use is explicitly prohibited
- Download or upload inappropriate, illegal or obscene material on a mobile phone using a corporate internet connection.

How to properly use mobile phones in the workplace

Employees can benefit from using mobile phones. They're allowed to use their phones:

- To make business calls.
- To use productivity apps.
- To check important messages.
- To make brief personal calls away from the working space of colleagues.

Disciplinary Consequences

Our company retains the right to monitor employees for excessive or inappropriate use of their mobile phones. If an employee's phone usage causes a decline in productivity or interferes with our operations, we'll ban that employee from using their mobile phones.

Employees may face severe disciplinary action up to and including termination, in cases when they:

- Cause a security breach.
- Violate our confidentiality policy.

Email Policy

Policy brief & purpose

Foveal LLP's email usage policy helps Partners and employees use their company email addresses appropriately. Email is essential to our everyday jobs. We want to ensure that our employees understand the limitations of using their corporate email accounts.

Our goal is to protect our confidential data from breaches and safeguard our reputation and technological property.

Scope

This policy applies to all Foveal LLP Partners (referred to as Partners hereon), employees and contractors who are assigned (or given access to) a Foveal LLP corporate email. This email may be assigned to an individual (e.g. employeename@foveal.net) or department (e.g. info@foveal.net.)

Policy elements

Corporate emails are powerful tools that help employees in their jobs. Employees should use their company email primarily for work-related purposes. However, we want to provide employees with some freedom to use their emails for personal reasons.

We will define what constitutes appropriate and inappropriate use.

Inappropriate use of company email

Our Partners and employees represent Foveal LLP whenever they use their corporate email address. They must not:

- Sign up for illegal, unreliable, disreputable or suspect websites and services.
- Send unauthorised marketing content or solicitation emails.
- Register for a competitor's services unless authorised.

- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their coworkers.

Our company has the right to monitor and archive corporate emails.

Appropriate use of corporate email

Employees are allowed to use their corporate email for work-related purposes without limitations. For example, employees can use their email to:

- Communicate with current or prospective customers and partners.
- Log in to purchased software they have legitimate access to.
- Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

Personal use

Employees are allowed to use their corporate email for some personal reasons. For example, employees can use their corporate email to:

- Register for classes or online Zoom/Teams meetings.
- Send emails to friends and family as long as they don't spam or disclose confidential information.

Employees must adhere to this policy at all times, in addition to our data protection guidelines.

Email security

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our equipment.

Employees must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
- Remember passwords instead of writing them down and keep them secret.
- Change their email password every three months.

Also, employees should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of clickbait titles.

- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can ask a Partner

Foveal LLP will keep their anti-malware programs up to date.

Email signature

Foveal LLP wil provide an email signature that exudes professionalism and represents our company well. Salespeople and executives, who represent our company to customers and stakeholders, should pay special attention to how they close emails. Here is a template the email signature:

Title Firstname Last name

Job Title
Foveal LLP

One Fleet Place, London, EC4M 7WS, UK
office: +44 203 6371 007¦ mob: +44 7903 313624

email:zzzz@foveal.net

Foveal LLP is authorised and regulated by the Financial Conduct Authority.

Disciplinary action

Employees who don't adhere to the present policy will face disciplinary action up to and including termination. Example reasons for termination are:

- Using a corporate email address to send confidential data without authorisation.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.
- Using a corporate email for an illegal activity.

Internet usage policy

Policy brief & purpose

Foveal LLP's internet usage policy outlines our guidelines for using our company's internet connection, network and equipment. We want to avoid inappropriate or illegal internet use that creates risks for Foveal LLp's legality and reputation.

Scope

This internet usage policy applies to all our all Foveal LLP Partners (referred to as Partners hereon), employees, contractors, volunteers who access our network and computers.

Foveal LLP internet usage policy elements

What is appropriate employee internet usage?

Our employees are advised to use our company's internet connection for the following reasons:

- To complete their job duties.
- To seek out information that they can use to improve their work.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet.

Any use of our network and connection must follow our data protection policy.

Employees should:

- Keep their passwords secret at all times.
- Log into their corporate accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

What is inappropriate employee internet usage?

Our employees mustn't use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorised recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorised or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask a Partner.

Foveal LLP has installed anti-virus software and firewalls on our company computers. Employees may not deactivate or configure settings and firewalls without managerial approval.

We won't assume any responsibility if employee devices are infected by malicious software, or if their personal data is compromised as a result of inappropriate employee use.

Company-issued equipment

We expect our employees to respect and protect our company's equipment. "Company equipment" in this computer usage policy for employees includes company-issued phones, laptops, tablets and any other electronic equipment, and belongs to our company.

We advise our employees to lock their devices in their desks when they're not using them. Our employees are responsible for their equipment whenever they take it out of their offices.

Email

Our employees can use their corporate email accounts for both work-related and personal purposes as long as they don't violate this policy's rules. Employees shouldn't use their corporate email to:

- Register to illegal, unsafe, disreputable or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorised advertisements or solicitation emails.
- Sign up for a competitor's services unless authorised.

Our company has the right to monitor corporate emails. We also have the right to monitor the websites that employees visit on our computers.

Disciplinary Action

Employees who don't conform to this employee internet usage policy will face disciplinary action. Serious violations will result in termination of employment or legal action, as appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our computers to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.