This template has been provided the Scottish Council for Voluntary Organisations (SCVO).

Use of this model policy is entirely at your own risk. The policy should be adapted to suit your own organisational needs, and you should ensure if meets your own specific requirements. You should also check this policy is compliant with the law and your organisation’s governing document. No liability rests with SCVO.

For more information see our information on [using SCVO templates](https://scvo.scot/support/using-scvo-templates).

Employee handbook - internet and email use

Note

The employee handbook, and the internet and email policies included in the handbook, should form part of the employee induction programme. These should be explained, in detail, to new starters and reinforced periodically to all staff through training sessions.

**Employers’ liability**

[INSERT DETAILS ON EMPLOYER LIABILITY FOR INFORMATION POSTED ONLINE AND SENT THROUGH EMAILS].

Note

Although posted online by an employee, employers remain liable for employees’ internet activity. Having an internet and email policy will be important to reduce liability, especially for any unlawful actions carried out by employees online. A policy will provide clear evidence of the employer’s stance on this issue and can be relied on in the future.

**Internet use (disregarding email)**

**Access**

[INSERT DETAILS ON EMPLOYEE INTERNET ACCESS].

Note

It should be outlined in the handbook which employees are permitted to access the internet, the individual or department they need to consult to receive access and the extent of their access i.e. whether this is solely for business purposes or whether personal use is permitted.

**Accessing inappropriate websites**

[INSERT DETAILS ON ACCESSING INAPPROPRIATE WEBSITES].

Note

It should be specifically outlined in the handbook that visiting inappropriate websites, carrying out inappropriate searches or downloading material which is deemed to be offensive, explicit or indecent is prohibited and may result in dismissal.

Any access to non-work-related websites, e.g. holiday booking or sport websites, should be outlined clearly in the handbook, including details on whether this access is permitted within working hours or should only take place outside working hours.

**Blogging**

[INSERT DETAILS ON BLOGGING ACTIVITY].

Note

Weblogs, commonly called blogs, are online journals or commentary hosted online.

It should be outlined in the handbook that employees who disclose confidential, sensitive or inappropriateorganisation information on a blog will be subject to disciplinary action.

Any organisation rules on accessing or updating blogs during working hours should also be outlined in the handbook,

**Reliance on information sourced online**

[INSERT DETAILS ON RELYING ON INFORMATION AND THE QUALITY OF INFORMATION SOURCED ONLINE].

Note

It is easy for employees to carry out internet searches and access vast amounts of information online.

It should be outlined in the handbook that information sourced online should be checked to ensure the information is current. It should also state that employees should check the accuracy, applicability and origin of the information before relying on this.

Any risks of using unregulated or inaccurate information should also be outlined.

**Breaching copyright laws**

[INSERT DETAILS ON BREACHING COPYRIGHT LAWS].

Note

Copyright laws cover information posted online. It should be outlined in the handbook that employees must not breach copyright laws by copying information off the internet without permission.

**Email use**

**Limitations on use**

[INSERT DETAILS ON ANY EMAIL LIMITATIONS].

Note

The extent of employee use of email facilities should be outlined in the handbook ie whether email is solely for business purposes or whether personal use is permitted. Any limitation will generally reflect similar organisation limitations e.g. limitations on personal use of the internet or use of organisation mobile phones.

**Content**

[INSERT DETAILS ON EMAIL CONTENT].

Note

Although sent by an employee, employers may remain liable for employees’ email activity.

It should be outlined in the handbook that any offensive, explicit or indecent email content is expressly prohibited and the sending of such content will lead to disciplinary action.

As written material, emails are subject to the same legal requirements as other written documents. Applicable laws should be outlined in the handbook and employees should be advised to ensure emails do not contain defamatory or inaccurate content.

Although disclaimers can be used on external emails, the requirement for employees to act responsibly and appropriately should be outlined. The handbook can also identify who the employee should speak to if they have any concerns with the contents of an external email.

**Effective use**

[INSERT DETAILS ON EFFECTIVE EMAIL USE].

Note

The use of emails aids productive communication but can lead to significant amounts of time lost if used inappropriately or overused.

It should be outlined in the handbook that emails should be used by employees effectively to communicate relevantmessages and any forwarding, or sending of, emails to large numbers of recipients should be limited as far as possible.

**Delivery**

[INSERT DETAILS ON DELIVERY OF EMAILS].

Note

To ensure the safe delivery of emails, it should be outlined in the handbook that care must be taken to ensure emails are correctly sent and any emails delivered to the wrong recipient must be redelivered correctly. It should also state that any information enclosed in a wrongly delivered message must not be accessed by the recipient.

Restrictions on revealing email address to others, internally and externally, should also be contained in the handbook.

**Housekeeping**

[INSERT DETAILS ON DELETING AND ARCHIVING EMAILS].

Note

Many businesses have organisation-wide email archiving and storage systems. The handbook can be used to outline any organisation guidance on deleting and archiving individual emails to ensure effective storage and inbox use.

**Disclaimers**

[INSERT INFORMATION ON DISCLAIMERS IN EMAIL].

Note

A disclaimer can be used on external documents to limit the organisation’s liability in cases where incorrect information is sent by email. The organisation may use a standard disclosure across all their written documents or have a specific email disclosure.

It should be outlined in the handbook which external emails are required to contain a disclosure and, if applicable, which disclosure statement must be used.

**Monitoring**

[INSERT DETAILS ON MONITORING INCLUDING EMAILS AND INTERNET USE].

Note

To ensure the effective running of the business, an organisation may legitimately decide to monitor internet and email use provided it is done so in accordance with data protection laws. This information should be included in your employee privacy notice to ensure transparency around data processing required by the GDPR and Data Protection Act.

In order to carry this out lawfully, employees must be informed in advance that monitoring is taking place. Outlining this in the handbook is likely to be sufficient and any monitoring clause can include information on what communication is monitored, when this is monitored, how monitoring is carried out and whether disciplinary action will be taken as a result of monitoring.

**Disciplinary action**

[INSERT DETAILS ON DISCIPLINARY ACTION].

Note

It should be outlined in the handbook that disciplinary action will be taken as a consequence of breaching the internet and email rules. A range of action is likely to be necessary dependent on whether the breach is accidental or deliberate and whether any information obtain is inappropriate or illegal etc.

**Security**

**Passwords**

[INSERT DETAILS ON EMPLOYEE PASSWORDS].

Note

Passwords provide an additional layer of security when used correctly.

It should be outlined in the handbook that employees are prohibited from revealing their password to others or allowing other users to use their equipment once logged in.

Any organisation rules on password requirements, frequency of renewing passwords and unlocking access should also be outlined.

**Malicious software**

[INSERT DETAILS REGARDING MALICIOUS SOFTWARE].

Note

Malicious software is an increasing threat to computer security and is becoming increasingly intelligent.

It should be outlined in the handbook that employees must take care when using email, whether any software downloading is restricted or forbidden unless permission is sought and the organisation’s procedure for reporting any suspicious software.

**Document version control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version number** | **Change or update** | **Author or owner** | **Date** |
| 1.0 | First version |  |  |
|  |  |  |  |
|  |  |  |  |