INTERNET AND E-MAIL

VERSION No	2
REVIEWED BY	Mariana Philipova
NUMBER OF PAGES	5

Policy Statement

Email and internet usage are an important part of effective communication and information gathering within the workplace. They can be a fast and reliable method of communicating both internally and with outside bodies such as family members, suppliers etc., therefore can have obvious significant advantages to our organisation. Email and internet usage is limited to legitimate business purposes only.

The purpose of the Internet and E-mail policy is to provide a framework to ensure that there is continuity of procedures in the usage of Internet and E-mail within the home. The Internet and E-mail system have established themselves as an important communications facility within the organisation and have provided us with contact with professional and academic sources throughout the world. Therefore, to ensure that we are able to utilise the system to its optimum we have devised a policy that provides maximum use of the facility whilst ensuring compliance with the legislation throughout.

Policy Aim

1. **Equipment and data security**: If you are issued with any equipment such as a laptop, mobile phone with email or internet access, personal data assistant (PDA,) etc., you should take all reasonable steps to ensure the safekeeping of both the equipment and any data either stored, or displayed on any such device.

- *If any such equipment is lost, damaged or stolen as a result of your negligence, we may deduct the cost, or partial cost, of the repair or replacement of any items, from any monies owing to you. We may also invoke the disciplinary process.*
- All data relating to our organisation, including that relating to any person in any way related to our organisation such as a customer or supplier etc. must not be stored on any equipment which does not belong to the organisation. If you are found to have done so you will be liable to disciplinary action.
- Care should also be taken to protect the data from being accessed or read by any unauthorised person. You should therefore ensure that your computer screen is switched off when away from your workstation. If you are accessing information from a mobile device, then care should be taken to ensure it cannot be read by anyone around you (e.g. if sitting in a cafe or on the train etc.) The Data Protection Code of Practice should be adhered to at all times when dealing with sensitive personal data.
- If passwords are issued, then you should not give your password to any other person, either within the organisation or external to it.
- Our email and internet systems may only be used by persons authorised to do so. Unauthorised access may result in disciplinary action.
- You must not modify any existing systems, programs, information or data without permission from a Director. When deleting any information, you should ensure that such a deletion could not have an adverse effect on the organisation or expose us to any risk.
- You are forbidden from downloading or installing any software from any source without express permission from a Director. This includes using USB flash drives, PDA, mobile phone etc.

2. **E-mail usage**

- Email can be used both to contact and pass information to others both formally and

informally.

- The use of the E-mail system is encouraged as its appropriate use facilitates efficiency. Used correctly it is a facility that is of assistance to employees.
- Inappropriate use however causes many problems including distractions, time wasting and legal claims.
- The procedure sets out the organisation's position on the correct use of the E-mail system.
- Care should be taken to ensure the most appropriate method of communicating with each party is used. You should remember that any offer or contract etc. is just as binding when sent by email as by any other way. The organisation's standard disclaimer should always be in evidence on emails sent by you.
- Care should be taken when transmitting personal, sensitive or confidential information. If you are unsure you should check if the recipients email address is confidential and that they know the nature of the information being transmitted.
- You should not breach any copyright or intellectual information when transmitting information.
- You should not send any inappropriate material to any party which could be deemed to be offensive, abusive, obscene, discriminatory, harassing, defamatory or derogatory, whether or not the recipient indicates they would not object. If you receive any transmission which you deem to be offensive or upsetting, you should immediately notify a Director.
- **Additionally, you MUST NOT:**
  - **Use the system for personal use**
  - **Send or forward chain mail, junk mail, jokes, gossip etc.**
  - **Use the system for trivial and unnecessary messages**

3. Procedures: Authorised E-mail Use:

a) Unauthorised or inappropriate use of the E-mail system may result in disciplinary action which could include summary dismissal.

b) The E-mail system is available for communication and matters directly concerned with the legitimate business of the organisation. Employees using the E-mail system should give particular attention to the following points:

i) all comply with the homes' communication standards;
ii) E-mail messages and copies should only be sent to those for whom they are particularly relevant;
iii) E-mail should not be used as a substitute for face-to-face communication or telephone contact. Flame mails (i.e. E-mails that are abusive) must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding;
iv) if E-mail is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The home will be liable for infringing copyright or any defamatory information that is circulated either within the organisation or to external users of the system; and
v) offers or contracts transmitted by E-mail are as legally binding on the organisation as those sent on paper.

c) The home will not tolerate the use of the E-mail system for unofficial or inappropriate purposes, including:

i) any messages that could constitute bullying, harassment or other detriment;
ii) personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);
iii) on-line gambling;
iv) accessing or transmitting pornography;
v) transmitting copyright information and/or any software available to the user; or
vi) posting confidential information about other employees, the organisation or its

service users or suppliers.

4. **Internet**

Where appropriate, duly authorised staff are encouraged to make use of the Internet as part of their official and professional activities. Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the name of the home. Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence. The intellectual property right and copyright must not be compromised when publishing on the Internet. The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal.

5. **Procedures: Internet usage / Acceptable / Unacceptable Use**:

a) Unauthorised or inappropriate use of the internet system may result in disciplinary action which could result in summary dismissal.

b) The internet system is available for legitimate business use and matters concerned directly with the job being done. Employees using the internet system should give particular attention to the following points:

i) Comply with all of our internet standards;
ii) Access during working hours should be for business use only;
iii)There should be no private use of the internet during normal working hours.

c) The organisation will not tolerate the use of the Internet system for unofficial or inappropriate purposes, including:

i) Accessing websites which put our internet at risk of (including but not limited to) viruses, compromising our copyright or intellectual property rights;
ii) Non-compliance of our social networking policy;
iii)connecting, posting or downloading any information unrelated to their employment and **in particular pornographic** or other offensive material;
iv)Engaging in **computer hacking and other related activities**, or attempting to disable or compromise security of information contained on the organisation's computers.

You are reminded that such activities (iii. and iv.) may constitute a criminal offence

⚠ When you visit websites, devices are often employed to enable the site owner to identify the source of the visit. It is therefore important that you only visit reputable sites which are necessary for the performance of your duties.

⚠ You must not visit any site or download any information which is illegal, immoral, offensive, abusive, obscene, discriminatory, harassing, defamatory or derogatory. If you have reason to believe any other employee is doing so, you should report your concerns to a Director as soon as possible.

⚠ You should not attempt to access any information which you know is restricted and you are not authorised to view.

3. **Monitoring:** The Organisation reserves the right to monitor all email and internet usage to ensure adherence to this policy regardless of whether the usage is during or outside of normal business hours. Subsequently any private usage should be authorised by a Director. We will monitor the use of our email and internet system, including where appropriate opening and reading emails (in line with Data Protection legislation). It is therefore important that you do not send any personal emails, particularly of a sensitive or embarrassing nature. We will monitor usage to ensure:

- The Organisation's policies, standards and guidelines are being followed
- To provide evidence of transmissions and communication
- To ensure there is no unauthorised usage

4. **Use of social media**

- You are forbidden from accessing social media for personal purposes whilst at work, whether on our computer equipment or your own (except during authorised breaks).

Social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums such as Twitter, Facebook and LinkedIn. Social media also covers blogs and video- and image-sharing websites such as YouTube and Flickr; however, this is not an exhaustive list. **ANYTHING ONCE OUT ON THE SOCIAL MEDIA CANNOT BE EVER REALLY DELETED AND IT IS FOR ALL TO SEE. PEOPLE HAVE LOST THEIR JOBS AND RUINED THEIR CAREERS!!!**

- We understand that many employees make use of social media in a personal capacity. While you are not acting on behalf of the Organisation, you must be aware that you can still damage the Organisation if you are recognised as being one of our employees.
- Whilst you are allowed to say that you work for us, and sometimes want to discuss your work on social media you must not make any derogatory comments regarding our business, other employees, management, suppliers, or any other person, business or other entity in any way connected to our business. This applies whether or not it is on our equipment or your own and if communicated in works time or your own time.
- Your online profile username (for example, the name of a blog or a Twitter name) must not contain the business' name.
- **You must not under any circumstances discuss your work on social media (for example, giving opinions on their specialism or the sector in which the organisation operates);**
- Any communications that you make in a personal capacity through social media must not:

a) Bring the Organisation into disrepute, for example by:

- criticising or arguing with people in their care or their family members, colleagues or rivals;
- making defamatory comments about individuals or other organisations or groups; or
- posting images that are inappropriate or links to inappropriate content;

b) Breach confidentiality, for example by:

- revealing trade secrets or information owned by the Organisation;
- giving away confidential information about an individual (such as a colleague or customer contact) or organisation (such as a rival business); or
- discussing the Organisation's internal workings (such as deals that it is doing with a [customer/client] or its future business plans that have not been communicated to the public);

c) Breach copyright, for example by:

- using someone else's images or written content without permission; or
- failing to give acknowledgement where permission has been given to reproduce something;

d) Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

- making offensive or derogatory comments relating to age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation, or perceived sexual orientation;
- using social media to bully another individual (such as an employee of the Organisation); or
- posting images that are discriminatory or offensive or links to such content;

e) Be of a nature which would cause us to lose faith in your integrity, or any of the people we care for or their family members to lose faith in the integrity of the Organisation.

5. To summarise:

- **You must not make any derogatory comments regarding our business, other employees, management, suppliers, or any other person, business or other entity in**

any way connected to our business. This applies whether or not it is on our equipment or your own and if communicated in works time or your own time.

You should also take care to limit who has access to view your comments or photographs etc. on such sites. Alternatively, if your behaviour is deemed to have brought the Organisation into disrepute, or caused any client, supplier, other business or any other entity connected to our business, to lose faith in the Organisation's integrity, you will be liable to disciplinary action, which dependent upon the circumstances, could lead to your summary dismissal.

6. **Mobile Devices:** Mobile devices, such as smart phones and tablet computers, are important tools for the organisation and their use is supported to achieve business goals.

   However mobile devices also represent a significant risk to information security and data security because if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organisation's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

   This organisation has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

7. **Scope:** All mobile devices, whether owned by this organisation or owned by employees, that have access to corporate networks, data and systems, not including corporate IT-managed laptops, this includes smart phones and tablet computers.

   Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted and authorised by security management.

8. **Technical Requirements**
   - Devices must use the following Operating Systems: Android 2.2 or later, 105 4.x or later.
   - Devices must store all user-saved passwords in an encrypted password store.
   - Devices must be configured with a secure password that complies with this organisations password policy. This password must not be the same as any other credentials used within the organisation.
   - With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

9. **User Requirements**
   - Users must only load data essential to their role onto their mobile device(s).
   - Users must report all lost or stolen devices to the IT manager immediately.
   - If a user suspects that unauthorised access to organisation data has taken place via a mobile device the user must report the incident to their manager
   - Continued failure to comply may lead to a disciplinary process.

10. **Training**

Training will be given to all staff using office based IT equipment to enable them to use it safely. All staff will be required to read this policy.

Related policies

Confidentiality
Cyber Security
Data Protection
Media and Public Relations
Mobile Phone Use
Monitoring and Accountability
Social Media and Networking