COMMUNITIES 1st
E-mail and Internet Usage Policy and Guidelines

Introduction

This policy sets out the obligations and expectations on volunteers and employees of Communities 1st, including affiliates, contractors and temporary staff, who use the organisation's IT facilities for internet and e-mail purposes. IT facilities are provided to assist with day to day work. It is important that they are used responsibly, are not abused, and that individuals understand the legal and ethical obligations that apply to them, as well as professional expectations. Whilst this policy covers both staff and volunteers, it is acknowledged that some clauses have more application to one group than the other.

Authorisation

No person is allowed to use the organisation's IT facilities who has not previously been authorised to do so. Unauthorised access to IT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

Legislation

All users shall comply with the relevant legislation. This includes the following:

General Data Protection Regulation (2016/679 EU)
Any information which the organisation holds is potentially disclosable to a requester under this legislation. This includes e-mails too.

Users need to be sure that they are not breaching any data protection when they write and send e-mails. This could include but is not limited to:

- Passing on personal information about an individual or third party without their consent.
- Keeping personal information longer than necessary.
- Sending personal information to a country outside the EEA.

E-mail should where possible be avoided when transmitting personal data about a third party. Any e-mail containing personal information about an individual may be liable to disclosure to that individual under the Data Protection Act 1998. This includes comment and opinion, as well as factual information. Therefore this should be borne in mind when writing e-mails, and when keeping them.

Computer Misuse Act 1990 - This Act makes it an offence to try and access any computer system for which authorisation has not been given.

Copyright Design and Patents Act 1988 - Under this Act it is an offence to copy software without the permission of the owner of the copyright.

Defamation Act 1996 - Under this Act it is an offence to publish untrue statements which adversely affect the reputation of a person or group of persons.

Terrorism Act 2006 - This Act has makes it a criminal offence to encourage terrorism and/or disseminate terrorist publications.

Regulation of Inventory Powers Act 2000 (RIPA) - Interception is authorised when there are reasonable grounds to suspect that the user has consented.

Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000. - This allows for any organisation to monitor or record communications (telephone, internet, e-mail, and fax) for defined business related purposes.

Responsibilities
All Users are expected to act in a manner that will not cause damage to IT facilities or disrupt IT services. Any accidental damage or disruption must be reported as soon as possible after the incident has occurred. Users are responsible for any IT activity which is initiated under their username.

Use of the Internet
Use of the Internet by employees and volunteers is encouraged where such use is consistent with their work or studies or with the goals and objectives of Communities 1st.

Reasonable personal use is permissible subject to the following:

- Users must not participate in any online activities that are likely to bring the organisation into disrepute, create or transmit material that might be defamatory or incur liability on the part of the organisation, or adversely impact on the image of the organisation.
- Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography), obscene matter, race hate material, violence condoning messages, criminal skills, terrorism, cults, gambling and illegal drugs.
- Users must not knowingly introduce any form of computer virus into the organisation's computer network.
- Personal use of the internet must not cause an increase for significant resource demand, e.g. storage, capacity, speed or degrade system performance.
- Users must not "hack into" unauthorised areas.
- Users must not download commercial software or any copyrighted materials belonging to third parties, unless such downloads are covered or permitted under a commercial agreement or other such licence.
- Users must not use the internet for personal financial gain.
- Users must not use the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.
- Users must not use the internet to send offensive or harassing material to other users.
- Use of the internet for personal reasons (e.g. online banking, shopping, information surfing) must be limited, reasonable and not distract from work duties.
- Use of social networking sites such as, but not limited to, Facebook, LinkedIn, Youtube, Twitter, Bebo, Flickr, MySpace etc is allowable so long as it is reasonable, proportionate and does not interfere with work duties. Access other than for legitimate organisational purposes, should be confined to breaks, lunch or other non-work periods, unless there is a specific work related need.
- In using social networking sites users should be mindful of the following:
  - Users should not post offensive and inappropriate pictures or comments, or anything that might cause embarrassment to the organisation, its employees, volunteers, partners, participants etc.
  - Users will be held accountable for any comments in which the organisation is identified or identifiable, for any breaches of copyright or any defamatory postings.
  - Employees and volunteers should avoid identifying themselves as working for the organisation unless they are representing it in some capacity. Where identification with the organisation is given (whether it be an employee or volunteer), personal blogs or other personal posts should contain disclaimers making it clear that the opinions expressed are solely those of the author and do not represent the organisation's views.
  - Employees and volunteers in particular should not give recommendations, endorsements or references for individuals, companies, partner organisations or

products if they are identifying themselves with the organisation in any capacity.

Staff and volunteers may face disciplinary action or other sanctions if they breach this policy and/or bring embarrassment on the organisation or bring it into disrepute. This applies whether use is made of the organisation's IT or their own.

Use of E-mail

E-mails sent or received on the e-mail system form part of the official records of Communities 1st; they are not private property. Communities 1st does not recognise any right of employees or volunteers to impose restrictions on disclosure of e-mails within the organisation. Users are responsible for all actions relating to their e-mail account/pc username and should therefore make every effort to ensure no other person has access to their account. Personal use of e-mail is permitted so long as it does not detrimentally affect the wider responsibilities and duties of employees and volunteers and are subject to the following:

- Personal use of e-mail must not disrupt the organisation's wider IT systems (e.g. the deliberate importation of any form of computer virus) or cause an increase for significant resource demand, e.g. storage, capacity, speed or degrade system performance.
- Personal use of e-mail must not harm the organisation's reputation, bring it into disrepute, incur liability on the part of the organisation, or adversely impact on its image.
- Seeking to gain access to restricted areas of the network or other "hacking activities" is strictly forbidden.
- E-mail must not be used for the creation, retention or distribution of disruptive or offensive messages, images, materials or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs or social background. Employees or volunteers who receive e-mails with this content from other employees or volunteers of the organisation should report the matter to their line manager or academic supervisor.
- Users must not send e-mail messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libellous or contain illegal or offensive material, or foul language.
- Users must not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- Users must not engage in any activity that is likely to:
  - Corrupt or destroy other users' data or disrupt the work of other users
  - Waste staff effort or organisation resources, or engage in activities that serve to deny service to other users
  - Be outside of the scope of normal work-related duties or studies – for example, unauthorised selling/advertising of goods and services
  - Affect or have the potential to affect the performance or damage or overload the Communities 1st's system, network, and/or external communications in any way
  - Be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights

Use of the organisation's e-mail system for personal e-mails is permitted but must be reasonable and limited and must not interfere with work or studies or those of other colleagues and individuals. Non-work related e-mail should be saved in a separate folder from work related e-mail.

Users should not send chain letters or joke e-mails from Communities 1st's email account/system.

Staff and volunteers, who receive improper e-mail from individuals inside or outside the organisation, should discuss the matter in the first instance with their line manager.

Good Practice
Where sensitive and confidential information needs to be sent via e-mail for practical reasons, please be aware that e-mail is essentially a non-confidential means of communication. E-mails can easily be forwarded or archived without the original sender's knowledge. They may be read by persons other than those they are intended for.

Users must exercise due care when writing e-mails to avoid being rude or unnecessarily terse. E-mails sent from Communities 1st may be interpreted by others as official statements. Users are responsible for ensuring that their content and tone is appropriate. E-mails often need to be as formal and business like as other forms of written correspondence.

Users should delete all personal e-mails and attachments when they have been read and should also delete all unsolicited junkmail. In the process of archiving e-mails, users should ensure inappropriate material is not archived.

All outgoing mail is filtered to detect and prevent a virus infection being sent from Communities 1st's equipment. The organisation reserves the right to introduce organisation-wide content checking if this is deemed appropriate.

The Communities 1st provides a current and up-to-date automatic virus checker on all networked computers. However, caution should be used when opening any attachments or e-mails from unknown senders. Users must best endeavour to ensure that any file downloaded from the internet is done so from a reliable source. It is a disciplinary offence to disable the virus checker. Any concerns about external e-mails, including files containing attachments, should be discussed with the Helpdesk.

Monitoring
All resources of Communities 1st, including computers, e-mail, and voicemail are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of the normal business activity then, at any time and without prior notice, the organisation maintains the right to examine any systems and inspect and review all data recorded in those systems. This will be undertaken by authorised staff (e.g. the Chief Executive). Any information stored on a computer, whether the information is contained on a hard drive, USB drive or in any other manner may be subject to scrutiny by Communities 1st. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists in the management of information systems.

Communities 1st subscribes to a third party checking service so that all incoming e-mail is filtered for the protection from e-mail virus infection and unsolicited junk mail (e.g. spam).