Email, Internet and IT Policy and Procedures

Ratified: 10th October 2013
To be reviewed: October 2015

Introduction

1. CREST Waltham Forest is a local voluntary sector organisation. It has a small number of employees and a larger number of volunteers. CREST needs to make the most of information technology (IT) which can be both effective and efficient. It wishes to do so safely, appropriately, and competently.

2. Aimed primarily at staff and volunteers, this Acceptable Use Policy comprises four parts:

- General Policy Statement;
- Email Guidance and Requirements (Annex A)
- Internet Guidance and Requirements (Annex B); and
- IT Competency Guidance and Requirements (Annex C).

3. Full account has been taken of advice on information and communications technology acceptable use policy published by the National Council for Voluntary Organizations in March 2012.

General Policy Statement

4. CREST will keep IT hardware and software upgraded to a reasonable standard, subject to constraints on finance, access to support, and logistics. Staff and volunteers are expected to have sufficient competence to enable them to carry out their normal role on appointment. That said, personal development is encouraged particularly where better use of an IT application will make it easier/quicker to carry out the role and meet objectives. Relevant support and training may be provided, particularly where a specific objective calls for it.

5. In turn, staff and volunteers are expected to make the most of IT. They are expected to do so exercising a duty of care. That is, essentially, to act reasonably, carefully and safely in relation to:

- communicating within the office and with partners/clients/funders;
- using hardware and software;
- storing data; and
- using IT for personal use.

6. If they have any concerns about their own use of IT, they should speak to their line manager. If they have concerns about that of their staff, it should be discussed and any action taken/agreed. If they have concerns about that of others (apart from technical competence) they should speak to their line manager.

7. Staff and volunteers need to appreciate that, apart from personal records and anything commercial-in-confidence, data on CREST's computers is relatively open. Also that nothing is secure in the way, for example, a large company or government department's network is secure.

8. To maximize the benefits of its computer resources and minimize potential liabilities, it is important that CREST staff and volunteers adhere to a policy. When using desk and laptop computers and peripherals provided by CREST, they must use these resources responsibly

9. They are given access to CREST IT and the network to assist them in performing their job. They should not have an expectation of privacy in anything they create, or receive. This would be unrealistic in any organization, and additionally, CREST line managers have the right to review any material at any time.

10. The following activities are strictly prohibited.

i. Sending or requesting or downloading material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate.

ii. Store or send commercial advertisements, solicitations, and promotions, other than in direct relation to CREST business. Also destructive programs e.g. viruses, and political information.

iii. Wasting resources, e.g. sending mass mailings or chain letters, printing large personal documents or multiple documents of any size, spending excessive amounts of time on the internet for personal purposes such as gaming or shopping or gambling during agreed working hours, engaging in online chat groups, otherwise creating unnecessary network traffic.

iv. Using or copying software in violation of a license agreement or copyright.

v. Deliberately providing data on clients or other CREST staff or volunteers to third parties outside of CREST (or outside of line management for CREST staff and volunteers) without their consent, apart from the police.

vi. Using a personal programme - available on the web or brought on disk or by email - or peripheral without the consent of the CREST General Manager (or his nominated IT coordinator who could be staff, volunteer or consultant).

vii. Fail to report to line manager anything relating to IT that could be dangerous to safety and health if it cannot be corrected easily by the staff member or volunteer concerned (e.g. trailing cables).

11. Paras 3 to 9 above may be amended or revised from time to time. Staff and volunteers will be provided with copies whenever this is the case.

12. Violations of this policy will be taken seriously and will result in disciplinary action. In very serious or repeated cases, termination of employment or voluntary agreement could result.

13. Further, more detailed, information and guidance is attached in the annexes.

CREST Management Committee, October 2013

Annex A

E-mail Statement and Guidance

13. E-mail provides an efficient means of communicating with colleagues and external contacts. There are many benefits including economy of time and effort. But common sense and good judgment must be used. To maximize the benefits and minimize potential liabilities to CREST and its people the following guidance should be used.

- **Employee's duty of care:** Use the same care in drafting email and other electronic documents as you would for any other written communication. In some cases E-mail may be inappropriate, e.g. where a signature is required, where an issue is contentious and needs discussing on the phone or face-to-face, and where CREST letterhead needs to be used to indicate authority for purpose.
- **Test:** Before preparing or sending a message ask yourself "is this the best way and time to communicate on this subject; and would a third-party think what I have said is appropriate?".
- **Data Protection Act:** There are Data Protection implications in the electronic transfer of information and files containing personal information. Email is governed by the Data Protection

Act in exactly the same way as other computer files. So, it and any CREST policy on Data Protection in place must be applied.

- **Inappropriate material:** As covered in the General Statement, material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent or requested by email.
- **Chain E-mail:** This is not to be initiated or forwarded in normal work hours.
- **Large attachments:** Photos, graphics, and large documents can take a considerable time to process and block senders', colleagues, and recipients access to the net. It may be more efficient to save them to disk and send them in the post, or print them and send them.
- **Altering attribution information:** Staff and volunteers should make it clear who they are and in what capacity they are communicating (using any house-style requested by CREST). If forwarding/using texts of others these should be attributed.
- **Limited privacy:** No computer system can guarantee total security and privacy; and in any case CREST business should be open to sharing, especially with line-managers (and CREST reserves the right to monitor all electronic communications). You should never expect your electronic communications to be either private or secure. E-mail may be stored indefinitely on any number of computers, including that of the recipient.
- **Replies:** Staff and volunteers will normally check their email daily (or arrange an automatic reply with alternative solutions for anything urgent). An acknowledgement should be sent if a full reply isn't possible. This is polite and applies to external and internal email, across hierarchical lines. On the other hand, the same standards cannot be guaranteed for external contacts; so if an issue is very urgent use the phone to at least check the message has been received.
- **Overuse:** If seems that somebody is over-using E-mail, the line-manager should discuss this with the colleague. E-mail meanwhile should not be ignored.
- **Virus detection:** Files from external sources, including disks brought from home and downloaded files, however reputable the source may seem, may contain dangerous computer viruses that could damage the computer network. All such material MUST be first scanned with CREST approved virus checking software. **If an employee suspects that a virus has been introduced onto the network, notify the CREST General Manager immediately.**
- **Use of encryption software:** This shouldn't be used without the authorization of line-management who will need to be able to access files. A case for its use will be required.
- **Email disclaimer footers:** Employees may on occasion, receive email with disclaimer footers attached. CREST policy is not to use them itself.

Annex B

Internet Statement and Guidance

In addition to E-mail, many staff and volunteers may be provided with access to the Internet ("the Net") to assist them in performing their duties. The Net (sometimes referred to as the Worldwide Web) can be a valuable source of information and research, but there are certain guidelines and policies that have to be followed.

- **Disclaimer of liability for use of Internet:** CREST is not responsible for material viewed or downloaded by users from the Net. Staff and volunteers are cautioned that many of these pages include offensive and inappropriate material

- **Accessing inappropriate sites:** You have a duty to conduct yourself in a manner that is appropriate to the culture, aims and objectives of CREST. Visiting web sites leaves a trail that the site owners can trace back to the originator and the resulting publicity from visits to inappropriate sites could be highly embarrassing to CREST and individuals. Such activities are likely to be considered as gross misconduct (see Para 9.i. in the General Statement, in particular). There may be occasions when some employees, in the course of their work for CREST, require to access otherwise undesirable web sites. In such cases, employees involved must clear this in advance with their line manager.
- **Games and entertainment software:** Employees may not use the Net to download games or other entertainment software, including screen savers, or to play games. Only games pre-loaded on to computers by CREST are permissible, but not in normal working hours.
- **Illegal copying:** Employees are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages and other material you may wish to download or copy. You may not agree to a license or download any material without prior permission of the General Manager or his nominated IT coordinator, regardless of whether a registration fee is or is not involved. If a fee is involved this too must be agreed in advance.

Annex C

IT Competence Statement and Guidance

Using computers is now as commonplace as using pen, paper, and calculator. Nonetheless the following should be taken into consideration.

- If computer useage is to be expected in a role it needs to be set out when recruiting.
- If a particular skill or depth of competency will be needed this should be set out, or in some cases made "desirable" then addressed through training if necessary.
- If a greater depth of competency becomes necessary in a role, or if roles change, this should be identified during one-to-one discussions as part of the regular appraisal process, if not when the change happens. Training and/or time for self-development should be made available.
- Competence in using computers includes the data protection act and any CREST policy that is in-place.
- It also includes health and safety, and knowledge of CTEST's health and safety policy. Under no circumstances should machines and peripherals be opened for repair/servicing/modification other than for user servicing such as loading paper and ink, or using connections such as USB slots.
- Food and drink should be kept away from keyboards and other IT equipment.
- A break of at least five minutes from using a computer should be taken every hour to rest your eyes. Screens should be head-height and viewed straight-on. Cables should be tidied away (if this is not possible the line-manager should be consulted).
- Until such time as CREST implements a system back-up process, any important records, documents, spread sheets or databases MUST be saved to external media regularly. (E.g. a USB stick, the Cloud or a DVD-RW.) Frequency should be discussed with your line manager.
- Passwords should be used to secure access to confidential data, e.g. staff or client records; or contracts drafted for signature but sent via E-mail. Passwords should be shared with your line-manager. Advice on setting passwords can be found at www.ncvo-vol.org.uk/advice-support/ict/managing-ict/acceptable-use-policy

- Economy should be a consideration. Avoid printing hard-copies of documents unless really necessary, and ask for them to be circulated rather than copy them to several individuals, unless time is pressing. Print double-sided as a rule. Use single-sided waste A4 again, for note-paper or printing on the reverse, unless the original document was confidential. Confidential waste should be shredded.
- Care should be taken to keep CREST laptop computers , USB drives, and optical media, out of sight in cars and on public transport; and it should be stored safely when taken home.