

## **Policy—internet, email and communications**

### **1 Introduction**

- 1.1 This policy outlines the principles and standards The Canada-UK Foundation requires those using our internet, email and other communications systems to observe. It also explains when The Canada-UK Foundation will monitor the use of those systems and the action The Canada-UK Foundation will take if the terms of this policy are breached.
- 1.2 The Canada-UK Foundation expects all of its electronic and computer facilities to be used in an effective and professional manner and encourages all staff to develop the skills necessary to do so. These facilities are provided by The Canada-UK Foundation for its own business purposes to assist its staff in carrying out their duties effectively. It is the responsibility of all staff to ensure that this technology is used for proper business purposes and in a manner that does not compromise The Canada-UK Foundation or its workforce in any way.
- 1.3 Professional integrity is central to The Canada-UK Foundation and it must characterise all our dealings. All staff should think about how their own image or that of The Canada-UK Foundation may be affected by how they use the internet and other electronic communication systems. The same professional ethical obligations apply to conduct in online and offline environments.
- 1.4 This policy applies to the use of The Canada-UK Foundation technology while at work and also when using The Canada-UK Foundation technology from outside work eg when accessing our systems remotely, using a The Canada-UK Foundation laptop or tablet when travelling and when using smartphones or other portable devices.
- 1.5 Misuse of the internet, email and/or other communication systems can expose both individuals and The Canada-UK Foundation to legal or financial liability.

For example, an individual may enter into unintended contracts, breach copyright or licensing arrangements, incur liability for defamation or harassment or introduce viruses into the system. This policy is designed to safeguard both individuals and The Canada-UK Foundation from such liabilities. It is important that all staff read the policy carefully and ensure that all use of the internet, email and other communication systems is in accordance with its terms. This policy should also be read in conjunction with The Canada-UK Foundation's other data protection policies.

- 1.6 This policy applies to all employees of The Canada-UK Foundation, trainees, consultants, contractors and all others who have access to The Canada-UK Foundation computer and other communications systems. It also applies to personal use of The Canada-UK Foundation's equipment and technology in any way that reasonably allows others to identify any individual as associated with The Canada-UK Foundation.
- 1.7 This policy does not form part of any employee's contract of employment and The Canada-UK Foundation may amend it at any time.

*[Executive Director]* is responsible for the monitoring and implementation of this policy. Any questions about the content or application of this policy or other comments should be referred to *[Executive Director]*

## 2 **Use of The Canada-UK Foundation's computer systems**

- 2.1 Staff may use The Canada-UK Foundation's computer systems only to the extent that they are authorised to do so. Staff should not use The Canada-UK Foundation's computer equipment for any purpose that is not connected to The Canada-UK Foundation's business unless they have express permission to do so or they are making personal use of the system as permitted by this policy (see paragraph 9).
- 2.2 Use of The Canada-UK Foundation's systems for commercial purposes other than the business of The Canada-UK Foundation is strictly prohibited.
- 2.3 Any individual with access to The Canada-UK Foundation's network must adhere to strict access controls, to reduce the risk of virus infections, hacking and other unauthorised access attempts:

- 2.3.1 only authorised equipment is allowed to connect to The Canada-UK Foundation's network from any office location;
  - 2.3.2 [remote access (via broadband, dial up, etc) is also restricted to authorised equipment and access must only be via secure means, eg VPN software;]
  - 2.3.3 the only access allowed to unauthorised equipment is via **Foundation owned electronics** and VPN.
- 2.4 The Canada-UK Foundation licenses software from a number of sources. The Canada-UK Foundation does not own that software and must comply with any restrictions or limitations on use, in accordance with its licence agreements. All staff must adhere to the provisions of any software licence agreements to which The Canada-UK Foundation is party.
- 2.5 Staff must not use any software for any purpose outside the business of The Canada-UK Foundation without express permission of [*Executive Director*] or as otherwise permitted by the terms of this policy.
- 2.6 Staff must not copy, download or install any software without first obtaining permission from [*Executive Director*].

### 3 **Confidentiality**

- 3.1 Staff should never assume that internal or external messages are necessarily private and confidential, even if marked as such. Email and the internet are not secure means of communication and third parties may be able to access or alter messages that have been sent or received. Do not send any information in an email which you would not be happy being publicly available. Matters of a sensitive or personal nature should not be transmitted by email unless absolutely unavoidable and if so, should be clearly marked in the message header as highly confidential. The confidentiality of internal communications can only be ensured if they are [sent by internal post, AND/OR delivered personally by hand AND/OR included in a password-protected or encrypted online document].
- 3.2 Email and internet messages should be treated as non-confidential. Anything sent through the internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way unless the messages are properly encrypted.

- 3.3 Staff should refer to The Canada-UK Foundation's data protection policies for details of the types of information that The Canada-UK Foundation regards as confidential and which should be treated with particular care.

#### 4 **General rules regarding communications and email**

- 4.1 All communications, including email, should reflect the highest professional standards at all times. In particular, all staff must:
  - 4.1.1 keep messages brief and to the point;
  - 4.1.2 ensure the spelling and grammar are carefully checked before sending;
  - 4.1.3 ensure that all emails sent from The Canada-UK Foundation include [the current disclaimer wording OR the following wording, *eg This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify our system manager by emailing admin@canadaukfoundation.org.*];
  - 4.1.4 ensure that an appropriate heading is inserted in the subject field; and
  - 4.1.5 double check the recipient(s) before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information about The Canada-UK Foundation or a customer.
- 4.2 Staff must not send messages from another person's email address (unless authorised in the proper performance of their duties) or under an assumed name.
- 4.3 Staff must not send offensive, demeaning, disruptive or defamatory messages or images by any method. This includes, but is not limited to, messages or images inconsistent with The Canada-UK Foundation's Equality Policy and Harassment and Bullying Policy and any sexist or racist material or any material which could be offensive on the grounds of a person's disability, age, sexual orientation, gender or religion or belief.
- 4.4 Staff must not place on the system or send any message or image which could be regarded as personal, potentially offensive or frivolous to any recipient or to any other person (even if not sent to them).
- 4.5 If any individual receives any communication containing material that is offensive or inappropriate to the office environment, the individual must delete it

- immediately. Under no circumstances should such communication be forwarded either internally or externally, other than internally to [*Chair of the Board and/or the Executive Director*] in order to report a breach of this policy.
- 4.6 Staff should not transmit anything in an email or other communication that they would not be comfortable writing (or someone else reading) in a letter. Emails leave a retrievable record and, even when deleted, can remain on both the individual's computer and on The Canada-UK Foundation's back-up system. Emails can be recovered and used as evidence in court proceedings and/or reviewed by regulators. Electronic messages are admissible as evidence in legal proceedings and have been used successfully in libel and discrimination cases.
- 4.7 Staff must not create congestion on The Canada-UK Foundation's systems by sending trivial messages or by unnecessary copying or forwarding of messages to recipients who do not need to receive them, or by sending or forwarding chain mail, junk mail, cartoons, jokes or gossip.
- 4.8 Staff must use a The Canada-UK Foundation email address for sending and receiving work-related emails and must not use their own personal email accounts to send or receive emails for the purposes of The Canada-UK Foundation's business. Staff must not send (inside or outside work) any message in The Canada-UK Foundation's name unless it is for an authorised, work-related purpose.
- 4.9 Staff must not send unsolicited commercial emails to persons with whom the individual does not have a prior relationship without the express permission of the relevant manager.
- 4.10 Communications must not use The Canada-UK Foundation's logos and other branding material without the approval of [*the Executive Director*].
- 4.11 [Communications must not provide references, recommendations or endorsements for any third party, unless expressly authorised by [*Executive Director*].]
- 4.12 [Emails will be for, stored on *The Canada-UK Foundation's server*] for , 1 year], after which they will be permanently deleted. If an individual wish to keep any emails beyond this date that are not customer-related, they should use their [ *personal folders*]. Any customer-related emails should be [printed and filed within 48 hours of receipt AND/OR attached to The Canada-UK Foundation's document management system within 48 hours of receipt].

- 5.1 Each individual is personally responsible for the security of all equipment allocated to or used by them. An individual must not allow equipment allocated to that person to be used by any other person other than in accordance with this policy.
- 5.2 Each individual must use passwords on all IT equipment allocated to them and must keep any password allocated to them confidential and must change their password regularly.
- 5.3 No individual may use another person's username and/or password to access The Canada-UK Foundation's systems, nor may any individual allow any other person to use their password(s). If it is anticipated that someone may need access to an individual's confidential files in their absence, that individual should arrange for the files to be copied to a network location that is properly secure where the other person can access them or give the person temporary access to the relevant personal folders.
- 5.4 All staff must log out of The Canada-UK Foundation's system or lock their computer when leaving their desk for any period of time. All staff must log out and shut down their computer at the end of the working day.

## 6 **Contact lists**

- 6.1 Lists of contacts compiled by staff during the course of their employment and stored on The Canada-UK Foundation's email system and/or other The Canada-UK Foundation database(s) (irrespective of how they are accessed) belong to The Canada-UK Foundation. Such lists may not be copied or removed by staff for use outside their employment or after their employment ends.

## 7 **Systems and data security**

- 7.1 Be vigilant when using The Canada-UK Foundation's email system. Computer viruses are often sent by email and can cause significant damage to The Canada-UK Foundation's information systems. Be particularly cautious in relation to unsolicited email from unknown sources.
- 7.2 If any individual suspects that an email may contain a virus, they should not reply to it, open any attachments to it or click on any links in it and must contact the IT department immediately for advice.
- 7.3 No individual may download or install software from external sources without prior authorisation from the *[Executive Director]*. OR Any files or software downloaded from the internet or brought from home must be virus checked

before use. Staff should not rely on their own computer to virus check any such programs but should refer direct to the IT department.

- 7.4 No personal computer, mobile phone, tablet computer, USB storage device or other device is permitted to be connected to The Canada-UK Foundation's systems or network without express prior permission from the [Executive Director]. Any permitted equipment must have up-to-date anti-virus software installed on it and The Canada-UK Foundation may inspect such equipment in order to verify this.
- 7.5 Staff must not run any '.exe' files, particularly those received via email, unless authorised to do so in advance by the IT department. Unauthorised files should be deleted immediately upon receipt without being opened.
- 7.6 Staff must not access or attempt to access any password-protected or restricted parts of The Canada-UK Foundation's systems for which they are not an authorised user.
- 7.7 All staff must inform the IT manager immediately if they suspect their computer may have a virus and must not use the computer again until informed it is safe to do so.
- 7.8 All laptop, tablet, smartphone and mobile phone users should be aware of the additional security risks associated with these items of equipment. All such equipment must be locked away in a secure location if left unattended overnight.

## 8 The internet

- 8.1 Access to the internet during working time is [strictly limited to OR primarily for] matters relating to your work duties and employment.[ Reasonable, limited personal use of the internet is permitted in accordance with paragraph 9.]
- 8.2 Any unauthorised use of the internet is strictly prohibited. Unauthorised use includes (but is not limited to):
- 8.2.1 creating, viewing, accessing any webpage or posting, transmitting or downloading any image, file or other information unrelated to your employment and, in particular, which could be regarded as pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to The Canada-UK Foundation or to our customers;

- 8.2.2 engaging in computer hacking and/or other related activities; and
  - 8.2.3 attempting to disable or compromise security of information contained on The Canada-UK Foundation's systems or those of a third party.
- 8.3 Staff are reminded that such activity may also constitute a criminal offence.
- 8.4 Postings placed on the internet may display The Canada-UK Foundation's address. For this reason, staff should make certain before posting information that the information reflects the standards and policies of The Canada-UK Foundation. Under no circumstances should information of a confidential or sensitive nature be placed on the internet. Staff must not use The Canada-UK Foundation's name in any internet posting (inside or outside work) unless it is for a work-related purpose.
- 8.5 Information posted or viewed on the internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the internet may be done only by express permission from the copyright holder. Staff must not act in such a way as to breach copyright or the licensing conditions of any internet site or computer program.
- 8.6 [Staff must not commit The Canada-UK Foundation to any form of contract through the internet [without the express permission of their manager].
- 8.7 Subscriptions to news groups, mailing lists and social networking websites are permitted only when the subscription is for a work-related purpose. Any other subscriptions are prohibited.
- 8.8 The Canada-UK Foundation may block or restrict access to any website at its discretion.

9 **Personal use of our systems**

- 9.1 Reasonable personal use of The Canada-UK Foundation's systems to send personal email, browse the internet and make personal telephone calls is allowed provided that it does not interfere with the performance of any individual's duties and the terms of this policy are strictly adhered to. The Canada-UK Foundation reserves the right, at our absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.
- 9.2 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

- 9.2.1 personal use must be minimal (both in terms of time spent and frequency) and reasonable and [must take place exclusively OR should take place mainly] outside normal working hours, ie during lunch or other breaks, or before and after work;
- 9.2.2 [personal emails must be labelled 'Personal' in the subject header [ and in the sensitivity settings];]
- 9.2.3 personal use must not affect the job performance of any member of staff or otherwise interfere with The Canada-UK Foundation 's business; and
- 9.2.4 it must not commit The Canada-UK Foundation to any marginal costs.[ Charges for personal telephone calls over a certain amount each month must be reimbursed to The Canada-UK Foundation in accordance with The Canada-UK Foundation's *[expenses policy]*.][ The Canada-UK Foundation's telephone system may not be used for premium rate or international calls[ unless expressly authorised by the individual's manager].]

- 9.3 [The Canada-UK Foundation does not permit access to web-based personal email such as Hotmail, Yahoo!, Outlook.com or Gmail on its systems at any time, due to the additional security risks to The Canada-UK Foundation's systems.]

## 10 Monitoring

10.1 The Canada-UK Foundation does not, as a matter of policy routinely monitor employees' use of the internet or the content of email messages sent or received. However, The Canada-UK Foundation has a right to protect the security of its systems, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon it. To achieve these objectives, The Canada-UK Foundation carries out random spot checks on the system which may include accessing individual email messages or checking on specific internet sites searched for and/or accessed by individuals. *[Insert any further statement explaining the purposes for which any monitoring is conducted, the extent of the monitoring and the means used for monitoring.]*

10.2 [The Canada-UK Foundation reserves the right to read any employee's emails in order to check for business emails while they are absent or out of the office. The Canada-

UK Foundation may also access any employee's voicemail to check for business calls while they are absent or out of the office. It may therefore be unavoidable that some personal messages will be read or heard.]

## 11 Prohibited use and breach of this policy

11.1 The Canada-UK Foundation considers this policy to be extremely important. Any breach of the policy will be dealt with under The Canada-UK Foundation's dismissal and disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in immediate termination of employment or engagement without notice or payment in lieu of notice. In addition, or as an alternative, The Canada-UK Foundation may withdraw an individual's internet and/or email access.

11.2 Examples of matters that will usually be treated as gross misconduct include (this list is not exhaustive):

11.2.1 unauthorised use of the internet as outlined in paragraph 8.2 above;

11.2.2 creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation;

11.2.3 creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other individuals, including material which breaches the principles set out in The Canada-UK Foundation's Equality Policy and our Harassment and Bullying Policy;

11.2.4 accessing, transmitting or downloading any confidential information about The Canada-UK Foundation and/or any of our staff and/or customers, except where authorised in the proper performance of your duties;

11.2.5 accessing, transmitting or downloading unauthorised software; and

11.2.6 viewing, accessing, transmitting or downloading any material in breach of copyright.

## 12 Review and training

- 12.1 The IT manager is responsible for this policy.
- 12.2 The Canada-UK Foundation regularly monitors the effectiveness of this policy to ensure it is working in practice and will review and update this policy as and when necessary. The Canada-UK Foundation will provide information and/or training on any changes made.
- 12.3 All staff will receive appropriate training on this policy, including training on any updates made to it.

I have read and understood this policy and agree to abide by its terms.

Signed \_\_\_\_\_

Date \_\_\_\_\_