IT POLICY

1 PURPOSE AND STATUS

1.1 Our electronic communications systems and equipment are intended to promote effective communication and working practices within the organisation, and are critical to the success of our business. This policy outlines the standards we require users of these systems to observe, the levels of privacy you can expect, the circumstances in which we will monitor use of these systems and the action we will take in respect of breaches of these standards.

1.2 This policy mainly deals with the use (and misuse) of computer equipment, email, internet, telephones, personal digital assistants and voicemail, but applies equally to use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards and all forms of digital information communication devices and related equipment.

1.3 Breach of this policy may be dealt with under our disciplinary procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach.

1.4 This policy is for guidance only and does not form part of your contract of employment (employees) or your volunteer agreement (volunteers) and may be amended at any time.

2 WHO IS COVERED

2.1 This policy covers all individuals working for us, including volunteers, at all levels and grades and regardless of status, working hours or place of work, including senior managers, officers, directors, employees, homeworkers, part-time and fixed-term employees, agency staff and contractors (collectively known as “you” in this policy), and also third parties who have access to our electronic communication systems.

3 IMPLEMENTATION OF POLICY

3.1 The Trustees have overall responsibility for this policy but have delegated day-to-day responsibility for overseeing and implementing action to the Chief Operating Officer. Responsibility for monitoring and reviewing the operation of the policy and any recommendations for change to minimise risks to our operations also lies with the Chief Operating Officer.

3.2 Managers have a specific responsibility to operate within the boundaries of this policy, to facilitate its operation by ensuring that you understand the standards of behaviour expected and in identifying and acting upon behaviour falling below these standards.

3.3 You should ensure that you take the time to read and understand this policy, and to disclose any misuse of our electronic communications systems which you become aware of to Operations@rafcf.org.uk. Questions regarding the content or application of this policy should also be directed to the Chief Operating Officer.

4 EQUIPMENT SECURITY AND PASSWORDS

4.1 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. If you are given access to the email system or to the internet, you are responsible for the security of your terminal(s). If leaving a terminal unattended it should be locked. On leaving the office, you should ensure that you log off to prevent unauthorised users accessing the system in your absence. Those without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting your Information Manager or the IT department.

4.2 Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Chief Operating Officer. For the avoidance of doubt, on the termination of

your employment (for any reason) or completion of your volunteer services, you must provide us with details of all your work-related passwords.

4.3 If you are issued with a Fund laptop or PDA, you must ensure that it is kept secure at all times. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the equipment is lost or stolen. You should be aware that if using equipment in public areas communications and documents may be read by members of the public. You must only access and/or deal with confidential or business sensitive matters in a suitably private environment. If you lose equipment issued to you, you may be liable to us for any losses. You should also observe basic safety rules when using such equipment, such as not using or displaying it obviously in isolated or dangerous areas. You must not use a "handheld" mobile telephone, PDA or similar device whilst driving. Use of mobile phones whilst driving is a criminal offence and will normally constitute gross misconduct.

5 SYSTEMS AND DATA SECURITY

5.1 You should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

5.2 You should not download or install software from external sources without authorisation from Operations@rafcf.org.uk. This includes programs, instant messaging programs, screensavers, photos, video clips and music files. Files and data should always be virus-checked by IT before they are downloaded. If in doubt, you should seek advice from Operations@rafcf.org.uk.

5.3 No device or equipment should be attached to our systems without prior approval from Operations@rafcf.org.uk. This includes any USB flash drive, MP3 or similar device, PDA or telephone. It also includes use of the USB port, infra-red connection port, Bluetooth connection port, Near Field Communication or any other port.

5.4 E-mails are monitored passing through the system for viruses. You should exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious (for example, if its name ends in .exe). The Operations department should be informed immediately if a suspected virus is received. We reserve the right to block access to attachments to emails for the purpose of effective use of the system and for compliance with this policy. We also reserve the right not to transmit any email message.

5.5 You should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

5.6 If you use laptops or Wi-Fi enabled equipment, you must be particularly vigilant about their use outside the office and take any precautions required against importing viruses or compromising the security of the system. The system contains information which is confidential to our operations and/or which is subject to data protection legislation. Such information must be treated with extreme care.

5.7 You are not permitted to store or copy any Fund files, information or data onto Dropbox, Amazon Cloud Drive or any other cloud-based storage system without written permission from Operations@rafcf.org.uk.

6 E-MAIL USE

6.1 E-mail is an important business tool which should be used with appropriate care and discipline. You should always consider if email is the appropriate medium for a particular communication. Messages sent on the email system should be written as professionally as a letter or fax. Messages should be concise and directed only to relevant individuals. Appropriate care must be taken to avoid unintentionally sending messages to an incorrect recipient, such as may arise by replying to all or where an addressee is suggested by the relevant address book. All emails of deemed importance should be filed in the relevant electronic filing system.

6.2 You should ensure that you access your emails regularly during any working day, stay in touch by remote access when travelling and use an out of office response when away from the office for more than a day.

6.3 You should take care with the content of email messages, as incorrect or improper statements can give rise to personal or Fund liability.

6.4 You must not send abusive, obscene, discriminatory, harassing, derogatory or defamatory messages whether internally or externally. If a recipient asks you to stop sending them personal messages always stop immediately.

If you receive such messages, they should not be forwarded and should be reported to the Chief Operating Officer. Where appropriate, the sender of the email should be referred to this policy and asked to stop sending such material.

6.5 If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via email, you should inform the Chief Operating Officer or the Chief Executive Officer who will usually seek to resolve the matter informally. If this informal response is unsuccessful, you should refer to the Fund's anti-harassment procedure.

6.6 You should not assume that internal or external messages are private and confidential, even if marked as such. The internet is not a 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 made publicly available. Matters of a sensitive or personal nature should be clearly marked in the message header as highly personal and confidential.

6.7 E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's mailbox or archives does not mean that an email is completely deleted and all email messages should be treated as potentially retrievable, either from the main server or by using specialist software.

6.8 You must ensure you are aware of and comply with paragraph 10 to ensure that your use of the Fund's equipment and systems is appropriate. By way of further guidance, in general, you should not:

6.8.1 Send or forward private emails at work which you would not want a third party to read;

6.8.2 Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the Fund;

6.8.3 Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them;

6.8.4 Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals;

6.8.5 Agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written in ink at the end of a letter;

6.8.6 Use the email system to copy and/or transmit any documents, software or other information protected by copyright laws, unless it is clear that the owner of such works allows this;

6.8.7 Send messages from another worker's computer or under an assumed name unless specifically authorised;

6.8.8 Send confidential messages via email or the internet, or by other means of external communication which are known not to be secure, unless the recipient has indicated they are happy to receive information in this way.

6.9 If you receive an email which has been wrongly delivered you should return it to the sender of the message. If the email contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way.

6.10 For our policy on personal use of our systems and equipment see paragraph 8 below.

7 INTERNET USE

7.1 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 unless the messages are encrypted.

7.2 You should also remember that text, music and other content on the internet are copyright works. Therefore, you should not download or email such content to others unless you are certain that the owner of such works allows this.

8 PERSONAL USE OF SYSTEMS

8.1 You are allowed to make reasonable and appropriate personal use of our internet, email, telephone systems and devices to send personal email, access the internet (including social media websites) make personal telephone calls or send other electronic messages subject to certain conditions set out below from our computers, networks and other IT resources and communications systems. However, this is provided this use is compliant with this policy at all times and does not interfere with your employment responsibilities or productivity. Our policy on personal use is a privilege and not a right and is dependent upon its not being abused or overused. We reserve the right to withdraw our permission or amend the scope of this policy at any time.

8.2 The following conditions must be met for personal usage to continue:

8.2.1 You should also not in any event spend a significant amount of time while at work using our communication systems for personal matters, whether telephone calls or social media websites, in a personal capacity or dealing with personal messages. As guidance, we would consider more than 30 minutes in a week outside formal breaks from work to be a significant amount of time.

8.2.2 Personal emails from your work account should be avoided, but minimal use is permitted. Any such email must be labelled “personal” in the subject header;

8.3 You should be aware that any personal use of the systems may also be monitored (see paragraph 9) and, where breaches of this policy are found, action may be taken under the disciplinary procedure. We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider that personal use is excessive.

9 MONITORING OF USE OF SYSTEMS

9.1 Our systems provide the capability to monitor telephone, email, voicemail, web and other communications traffic. For business reasons, and in order to perform various legal obligations, use of our systems including the telephone and computer systems, and any personal use of them (including emails marked “personal”), is continually monitored by the use of automated software. Monitoring will only be carried out to the extent permitted or required by law and as necessary and justifiable for business purposes.

9.2 We reserve the right to retrieve the contents of messages (including emails marked “personal”, “confidential” or any equivalent phrase) or details of any internet activity for the following purposes (this list is non-exhaustive):

9.2.1 to monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;

9.2.2 to protect the system against viruses or hackers;

9.2.3 to find lost messages or to retrieve messages lost due to computer failure;

9.2.4 to assist in the investigation of wrongful acts;

9.2.5 to combat or investigate fraud or corruption;

9.2.6 to comply with any legal obligation;

9.2.7 to protect our legitimate interests and activities.

9.3 The contents of any downloaded information, email or voicemail so obtained by us in the exercise of these powers may be disclosed without your permission.

9.4 All such records and data may be used as evidence in disciplinary proceedings or for any other legitimate purpose required by us.

10 INAPPROPRIATE USE OF EQUIPMENT AND SYSTEMS

10.1 Access is granted to the internet, telephones and to other electronic systems and equipment for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with paragraphs 7, **Error! Reference source not found.** and 8.

10.2 Misuse or abuse or inappropriate use of communication or related devices in breach of this policy will be dealt with in accordance with our disciplinary procedure. Misuse of the internet and communication devices can, in certain circumstances, constitute a criminal offence. In particular, misuse of the email or any messaging system or inappropriate use of the internet by viewing, accessing, transmitting, forwarding or downloading any of the following material, or engaging in any of the following activities, will amount to gross misconduct (this list is not exhaustive):

10.2.1 pornographic material (that is, writings, pictures, films, video clips of a sexually explicit or arousing nature); or

10.2.2 criminal material; or

10.2.3 any material which is liable to cause embarrassment to the Fund or to its clients; or

10.2.4 a false and defamatory statement about any person or organisation; or

10.2.5 material which is discriminatory, harassing, obscene, offensive, abusive, derogatory or may cause embarrassment to others; or

10.2.6 confidential information about the Fund, any of its staff or clients, contacts and/or suppliers; or

10.2.7 any other statement which is likely to create any liability (whether criminal or civil, and whether for you or the Fund); or

10.2.8 computer hacking and other related activities; or

10.2.9 disabling or attempting to disable or compromise the security of information contained on the Fund's computers; or

10.2.10 material in breach of copyright; or

10.2.11 online gambling; or

10.2.12 chain letters.

Any such action will be treated very seriously and is likely to result in summary dismissal.

10.3 Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our disciplinary procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the disciplinary procedure. If necessary such information may be handed to the police in connection with a criminal investigation.

11 COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

11.1 Our electronic communications systems and equipment should never be used in a way that breaches any of our other policies including our disciplinary policy, anti-harassment and bullying policy, equal opportunities policy, data protection policy or to breach our obligations with respect to the rules of any relevant regulatory bodies.

11.2 Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.