1.1 Electronic Mail (Email) and Internet Access

To ensure lawful and appropriate access and use of the RFDS Central Operations Email system and Internet access.

SCOPE
These policies apply to any person who accesses or has the opportunity to access the RFDS Central Operations Email system/Internet.

POLICIES
General
Email facilities and Internet are provided by the RFDS to enhance the communication and information processes of our organisation.

All facilities, equipment and material remain the property of the RFDS. Staff access to these facilities is provided for business use in accordance with this policy.

Email Use
Email resources are provided for **business use** in accordance with the following:

Email is company property.

Regardless of perception, emails are considered to be a written communication, even if stored electronically. This means that emails are subject to the same laws of defamation, harassment, discrimination, copyright and privacy that relate to written communications.

All use must be appropriate and lawful.

RFDS accept a reasonable amount of personal use of these facilities. However, such use **must not** interfere with an employee's ability to perform their job or if the person is not an employee, their obligations to the RFDS.

Misuse may damage our corporate and business image, and intellectual property generally, which can result in legal proceedings being brought against the employee and/or the RFDS.

Improper statements can give rise to liability - personally and for the RFDS:

- Work on the assumption that messages may be sent, forwarded or transmitted to someone other than who you intended to receive or read your message.
- Controlled or limited distribution of your messages cannot be guaranteed. It is unlawful to be a party to or to participate in the trafficking of any defamatory message.

- Likewise, do not send pornographic, provocative, offensive, abusive, sexist, or racist messages and do not forward them to others. This includes the transmission of jokes, anecdotes, song lyrics, animated and graphic images, and 'chain letters'.

Inappropriate or unlawful use will lead to disciplinary action.

Identity
Signatures and disclaimers are managed centrally and applied to all outgoing email

Email Security
RFDS reserves the right to monitor an individual's incoming and outgoing-email traffic, in particular when there is a suspicion that sending and receiving emails constitutes unlawful conduct.

The content of emails can be monitored and staff should be aware that emails are stored on the server. Our network logs include the email addresses of senders and recipients, and the time of transmission.

Emails will be accessed in the event of potential risk to the security of the network, or where the RFDS could be exposed to legal liability. RFDS will disclose the contents of emails and logs to a third party on a question of law or on production of legal authority.

If staff receive any suspicious or objectionable material they should advise their Senior Manager who should immediately advise the IT Manager.

Email Restrictions
Some to restrictions apply to size of messages that can be sent and overall mailbox size. If any issues/questions contact IT Manager.

Some file types are also blocked to protect our network. You will receive an automated alert if any of your messages are blocked in this way.

Confidentiality & Privacy
Do not send private, sensitive or highly confidential messages via the RFDS Central Operations Email system. You should not send anything by email that you wouldn't want a third party reading.

Most email is insecure and should be regarded as such unless it has been encoded or encrypted. Email messages are perceived to be instant in nature and disposal. They are retained by both the recipient and the sender until specifically disposed of into a recycle bin.

However, there is also an additional back up facility that retains email messages for a period of time on the RFDS central Operations network.

IT Policy

Network Access
Senior Managers must have any new staff members submit a completed 'IT Systems Access Form' to the IT Manager before the user will be able to access the RFDS email system.

When a staff member leaves the organisation, a "IT Systems Access Form' will be completed by the Payroll Officer and submitted to the IT Manager. It is the IT Manager's responsibility to then remove the staff member from the RFDS Central Operations computer systems.

Internet Use
All use must be appropriate and lawful.

You are prohibited from accessing from the Internet, or any other site, any material that is pornographic, objectionable or offensive. You must also not attempt to use the RFDS internet gateway to illegally 'hack' into another computer network.

Misuse may damage our corporate and business image and intellectual property generally, which can result in legal proceedings being brought against the employee and/or the RFDS.

RFDS accept a reasonable amount of personal use of these facilities.

However, such use **must not** interfere with an employee's ability to perform their job or if the person is not an employee, their obligations to the RFDS.Access to the Internet is provided by the IT Manager, at the discretion of the employee's senior manager

Staff access to the internet and any use of dial-up/out of normal hours (remote) access to the RFDS computer network is to be closely monitored and permitted for only authorised staff.

Security
The IT Manager and General Manager, Corporate Services are the only persons authorised to access logs and content of Internet browsing activities.

Internet browsing logs will be accessed in the event of potential risk to the security of the network, or where the RFDS could be exposed to legal liability.

Copyright
Not all information on the Internet is in the public domain or freely available for use without proper regard to rules regarding property rights (including copyright). Much of the information is subject to copyright protection under Australian law and by Australia's signature to international treaties, protected at international levels too.

"Use" includes downloading, reproducing, transmitting or in any way duplicating all or part of any information (text, graphics, videos, cartoons, images, sounds or music)

which is not in the public domain. Simply because material is available to view via the Internet, it is not necessarily in the public domain.

Virus Checking
All internet file downloads are checked for viruses. System logs record details of intercepted viruses, where they originated, and what actions were taken to quarantine/eliminate them.

To help contain the spread of computer viruses, staff members must not load any unauthorised copies of computer software onto the computer they use. Authorisation for software installation must be gained from the IT Manager before any software is installed.

1.2 IT Hardware and Software

PURPOSE
To record and control the details, location and warranty information of the RFDS Central Operations IT hardware assets.

SCOPE
These policies apply to any person who uses RFDS Central Operations personal computer hardware, either within existing RFDS Central Operations facilities or when working off-site, e.g. at home, when absent on duty, etc.

DEFINITIONS

IT Asset Register
A register of purchase details, specifications and current locations of all IT assets held by RFDS Central Operations.

Peripheral Equipment
All items of equipment that connects to or interact with personal computers and File Servers in use at RFDS Central Operations.

Personal Computer
In this document, the terms Personal Computer and PC are interchangeable. Also included are laptop PCs, hand-held data capture devices and all other personal/portable computing devices.

BACKGROUND
The RFDS Central Operations continues to make a significant investment to provide commercially viable computing facilities for staff:

Initially to acquire the network servers, communications equipment and personal computers, and

Ongoing to further enhance its IT facilities and support users who regularly connect to the network.

It is therefore essential that this investment is appropriately managed.

POLICIES

General
All IT related negotiations with external suppliers will be initiated by the IT Manager (as directed by the General Manager, Corporate Services), unless there is an urgent need or a remote location makes this impractical. (Under these circumstances full details of all purchases, including copies of invoices and serial numbers must be forwarded by the responsible Senior Manager to the IT Manager as soon as practicable after the transaction is complete.)

Full details of all purchases must be promptly recorded on the RFDS Central Operation's IT Asset Register, upon receipt of goods, which is maintained by the IT Manager.
The General Manager, Corporate Services must approve all personal computer purchases prior to purchase.
All personal computer purchases are to include licence(s) for appropriate operating system software.

Where an item is purchased as a replacement for a device to be written off, the old device must be returned to Adelaide Office (and marked for the attention of the IT Manager) for reallocation or disposal.

The specifications of personal computers and other devices to be purchased will be negotiated between the IT Manager and the appropriate staff member's Senior Manager.

Furthermore, the widespread use of personal computers within the RFDS exposes the organisation to risks at a number of levels:

- the risk of prosecution associated with illegal use and copying of software.
- the frustration associated with using different versions of the software.
- the risk of communication problems resulting from the connection of non-standard and diverse pieces of computer hardware to the network.

When any licensed software is installed on a personal computer the user is immediately responsible to the authors/developers of the software to protect the Intellectual Property resident in their software.

These responsibilities are specified in national and international agreements, and encompass unauthorised copying and illegal/unlicensed use. Penalties for breaches of these agreements are significant. It is therefore essential that this investment, its associated risks and responsibilities be appropriately managed.

Responsibility of IT Property
All IT equipment provided for staff use (e.g. desktop or laptop computers), remain the property of the RFDS Central Operations. The IT Manager has overall responsibility for the provision and maintenance of the equipment.

Each individual staff member is responsible for the security of the equipment they use. They are also to ensure the equipment be used and maintained in a responsible manner at all times.

Any cost of damage, loss or theft of IT hardware caused by an individual's negligence will be borne by the individual and not the organisation. Where the use of a laptop computer is no longer required by a particular staff member, it should be returned to their respective Senior Manager who will return it to the IT Manager where applicable.

Administration of Hardware Assets
The IT Manager is to maintain the RFDS Central Operations IT Asset Register, which lists details of all computer hardware owned by the organisation. This will be centrally located at the Adelaide Office.

All personal computers (including standalone units, networked terminals, laptops and hand-held devices) are to be loaded with or protected by a currently approved anti-virus solution. (As detailed in the RFDS Central Operations IT Software Policy).

PROCEDURE
Hardware and Software Purchases
All requests for computer hardware/software, either new or upgrades must initially be made by a Senior Manager to the IT Manager via email. Quotes from appropriate suppliers will be obtained and forwarded to the relevant manager for approval.

Upon approval a Purchase Order form is to be submitted to the IT Manager for action. No order will be placed without an appropriate purchase order.

All hardware purchases are to be received at the Adelaide Office where the IT Manager will apply an asset sticker and record the required details in the IT Asset Register.

Any setup or modification of the hardware (e.g. Software installation) will then take place before the hardware is dispatched to the required location.

If the need arises to have any purchased equipment delivered direct to a remote site, the Senior Manager of that site must liaise with the IT Manager to ensure an appropriate Asset sticker is supplied and the correct recording of asset details is completed.

Staff and Hardware Movements
When a staff member moves locations within RFDS Central Operations the employee's Senior Manager is to advise the IT Manager via email of their new location, to ensure the change of asset usage is recorded.

Any changes to the location or configuration of personal computers, portable/hand-held devices and other computer equipment must be promptly notified to the IT Manager on the same form or via email, to ensure the IT Asset Register is updated.

Software Installation
Software installation must be undertaken by the IT Staff.

No software is to be copied or installed on more than one personal computer unless the software licence permits such duplication and the IT Manager has approved the installation.

No software is to be installed on any RFDS personal computer unless that software is also owned/licensed for use by the RFDS and been approved for installation by the IT Manager. This includes but is not limited to:

- Software supplied free of charge by customers or suppliers;
- Software downloaded from the Internet; or
- Software received unsolicited via email or other similar means.

During the installation process, all software is to be registered in the name of 'RFDS Central Operations'. Where necessary, the registration process should specify both a username and company name as 'RFDS Central Operations'.

1.3 Network Access & Security

PURPOSE
To establish the policy & procedure for user access and security to the RFDS Central Operations Wide Area Network (WAN).

SCOPE
These policies apply to any person who accesses or has the opportunity to access the RFDS network.

DEFINITIONS

Username	Is a user specific identity that provides the means to access the RFDS network.
Password	Is a user defined personal access code to the RFDS network.

IT Policy

POLICIES

User
Every user is responsible for all network activity (e.g. transactions processed, emails sent and received, websites browsed) under their Username and Password.

User passwords are to consist of a minimum five (5) characters and should include both numbers and letters wherever possible.

Passwords are prompted to be changed automatically by the system every 60 days and the new password cannot be the same as the previous 5.

Usernames and passwords are not to be transferred between employees upon the termination of employment.

In order to protect the integrity of all RFDS data and to minimise occurrences of illegal system access, staff should ensure that they lock their workstation when they are likely to be absent from their work location for more than a few minutes.

To help maintain the security of the network, Usernames and Passwords must not be supplied to or used by other employees or third parties. (Users may need to divulge their password to the IT Manager on request, but the password must remain confidential at all times.). Users should seek help from the IT Manager to change their password if they suspect that it may be known by other staff.

Access rights to network resources are provided in line with an employee's specific role & responsibilities within RFDS Central Operations.

General
As part of their work functions, virtually all staff members need regular access to computer systems installed within RFDS Central Operations. The nature of the information contained within these systems requires that access to both the physical system(s) and the data within each system is well managed. Failure to do so may result in:

- loss or damage to data,
- disruption to services,
- breaches of (patient) confidentiality,
- financial loss to the organisation.

Inappropriate use of RFDS computer equipment that permits illegal and unauthorised access to its computer systems exposes the organisation to risks at a number of levels:

- the risk of disclosure resulting from uncontrolled access to information
- the opportunity for accidental data and/or financial loss
- the opportunity for malicious data destruction, and
- (Ultimately) being unable to meet its contractual obligations for the delivery of agreed aero-medical services to its clients.

The provision of 'Remote Access' facilities to staff and affiliated organisations has the potential to further exacerbate this situation because it provides further opportunities for uncontrolled or unauthorised access to computer systems at RFDS Central Operations.

All use of RFDS computer facilities must be appropriate and lawful. Misuse may damage our corporate and business image and intellectual property generally, which can result in legal proceedings being brought against the employee and/or the RFDS. The RFDS accepts a reasonable amount of personal use of these facilities. However, such use must not interfere with an employee's ability to perform their job or if the person is not an employee, their obligations to the RFDS.

The use of all RFDS computer systems (including in-house and remote access) is conditional on the staff member complying with all applicable IT Policies & Procedures including:-

- Network Access & Security, i.e. this document
- Electronic Mail (Email) Access & Security
- Internet Access & Usage
- IT Hardware
- IT Software

Failure to comply with the above policies may result in access being restricted or revoked and disciplinary action taken.

As the performance of the RFDS internet connection can fluctuate, the RFDS cannot guarantee a consistent level of service or permanent availability, either for in-house or remote system users.

Computer system users are strictly forbidden from attempting to access (i.e. 'hack' into) other RFDS systems or the systems of any other organisation (or individual) to which they have not been granted explicit access.

RFDS staff and other authorised computer systems users have been provided with access to confidential and/or privileged information. All such data/information and equipment remains the property of RFDS Central Operations, and every care should be taken to secure such material against loss, theft or disclosure.

Remote Access
If remote access is required contact the IT Department.

1.4 Recording of Telephone Calls

Incoming and outgoing telephone calls from RFDS' Tasking Centre in Port Augusta and the Triage Flight Nurse office at Adelaide Airport are monitored and recorded for service quality, compliance and security purposes.

Calls will be retrieved and/or monitored:

- For staff training and development;
- During the course of quality audits to ensure that RFDS and regulatory service and agreed contract standards of our partners are being met;
- If there is a threat to the health and safety of staff or any member of the public and/or for the prevention or detection of crime;
- When it is necessary to check compliance with regulatory procedures;
- If the RFDS is required to respond to or provide evidence for, investigations relating to particular patient incidents, eg coronial inquests etc;
- In the course of investigating internal or external complaints.

Personal data collected in the course of recording activities will be treated confidentially and stored securely.

1.5 Help Desk Facility

PURPOSE
To establish the policy & procedure for the provision of a 'Help Desk' facility to all RFDS Central Operations IT users.

SCOPE
These policies apply to any person who accesses or has the opportunity to access the RFDS network.

DEFINITIONS

Help Desk	Is a facility external of RFDS and provides a assistance to employees experiencing difficulties with the wider IT system.

POLICIES
A Help Desk facility operates at RFDS Central Operations to facilitate and provide remedies to all IT users experiencing IT difficulties.

PROCEDURE

1. IT users experiencing IT related difficulties should in the first instance ring the help desk on 08 8238 3338 for assistance;
2. Where the help desk is unable to provide assistance in a reasonable time users should contact the IT Manager