



South Yorkshire Fire & Rescue

WORKING FOR A SAFER
SOUTH YORKSHIRE

Acceptable Use Policy for Laptops

CONTENTS

Section	Title	Page No.
1	Purpose	1
2	Eligibility	1
3	Staff Responsibility	1
4	Care of Laptops	1
5	Transporting Laptops	2
6	Screen Care	2
7	Battery Use	2
8	Extreme Temperature, magnetic fields and x-ray	2
9	Security and Storage	2
10	Laptops left in unsupervised areas	2
11	Air Travel	3
12	Acceptable Use	3
13	Unacceptable Use	3
14	Viruses	3
15	Staff Absence	3
16	Staff leaving SYFR	4
17	Internet/E-mail and Wireless Connectivity	4
18	Personal Use	4
19	Technical Support	4
20	Insurance	5
21	Monitoring	5

South Yorkshire Fire and Rescue

Acceptable Use of Laptops Policy

1. Purpose

The purpose of this policy is to outline the acceptable use of laptops by South Yorkshire Fire and Rescue staff. As laptops will be used to access the ICT network, this document must be read in conjunction with SYFR's Security Policy.

Inappropriate use of laptops may expose SYFR to unnecessary risks including virus attacks, compromise of network systems and services, financial and legal issues. Therefore, this policy aims to:

- Guard against theft of the laptop
- Theft of the information stored on the laptop
- Damage to the equipment
- Promote appropriate use of the laptop computer

2. Eligibility

Providing that resources are available, permanent members of staff will be issued with a laptop at the discretion of SYFR management if it is felt necessary for them to carry out their duties.

Staff will only be provided with a laptop following submission of a FS 601 which has been duly authorised.

The appropriate and secure use of laptops will be monitored. Staff will be kept updated with any new developments and receive appropriate training for new or upgraded applications.

Every user who is issued with a laptop will be asked to sign for receipt of the portable device, and to acknowledge that they have read, understood and will comply with this policy.

3. Staff Responsibility

Staff should take good care of the laptop and take all reasonable precautions to ensure that it is not damaged, lost or stolen. In the event that the device is stolen, staff will be expected to report the theft to the police and obtain an incident number.

Staff members must report the loss of a laptop to their line manager who will subsequently inform ICT Section. Negligence in the care of laptops or failure to report loss or damage at the earliest opportunity may result in disciplinary action being taken against the staff member concerned.

4. Care of Laptops

A laptop is allocated to a particular member of staff for his or her use and is entrusted to their care. The member of staff should therefore take all reasonable care to secure the laptop and to guard against damage.

5. **Transporting Laptops**

Laptops should always be within the protective bag supplied with the laptop when carried.

The carrying case can hold objects (such as folders and books), but these must be kept to a minimum to avoid placing too much pressure and weight on the laptop screen.

For short periods of time i.e. moving between meetings, laptops may be put into hibernation (standby mode), thus reducing the start-up time. For longer periods, laptops should be turned off properly before placing it in the carry case.

Care should be taken when placing the laptop in overhead storage compartments e.g. when travelling by train/air to ensure that the laptop is secure and cannot slide around.

6. **Screen Care**

The laptop screen can be damaged if subject to rough treatment. The screen is particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the laptop when it is closed.
- Do not place anything in the carrying case that will press against the cover.
- Do not place anything on the keyboard because forgetting objects on the keyboard and closing the lid may cause damage to the screen.
- Only clean the screen with soft, dry cloth or anti-static cloth.

7. **Battery Use**

In order to prolong battery life, laptops should be powered from the mains supply whenever practical. General information on maintaining battery efficiency is available from ICT Section.

8. **Extreme Temperature, magnetic fields and x-ray**

Do be aware of the damage extreme temperature, magnetic fields and x-ray can cause to computers

9. **Security and Storage**

Each laptop's serial number will be recorded in the SYFR inventory of computer equipment database.

10. **Laptops left in unsupervised areas**

The user must take appropriate security measures to protect the laptop and all its peripherals. When unattended, the laptop must be stored in a secure locked location.

- Laptops must not be left in unsupervised areas. Unsupervised areas include unlocked offices. Do not leave a meeting or conference room without your laptop. Take it with you.
- Do not leave the laptop in an unlocked vehicle; even if the vehicle is in your driveway or garage.
- Never leave you laptop in plain sight. If you must leave you laptop in a vehicle, the best place is in the boot.
- Car parks are likely areas for thefts from vehicles as they provide wide choice and cover for thieves. Again, never leave your laptop in plain sight.

11. Air Travel

Laptops must be returned to ICT support to disable the wireless network adapter before travelling by air with the laptop.

When travelling by air, the laptop must be taken into the cabin. Do not check the laptop in as hold baggage.

It is safe to put the laptop through an x-ray security machine, but the laptop must never be put through a metal detector. Security staff may request that the laptop is removed from the carrying case to be inspected more closely.

12. Acceptable Use

Laptops and portable devices owned by SYFR are subject to the same policies and regulations as desktop machines.

Files should not be stored on the hard drive of the laptop. Files should be transferred to the network drive at the earliest opportunity. Local copies of confidential files should be deleted from the hard drive once they have been transferred. No responsibility will be taken if files that solely exist on the hard drive are lost due to mechanical failure or accidental deletion.

13. Unacceptable Use

Laptops must not be used by non SYFR employees. ICT must be informed if a laptop is loaned to another member of staff within SYFR.

14. Viruses

Laptops are configured to update the anti-virus on startup when connected to the SYFR network. The machine will run a local copy of anti-virus when being used as a stand-alone machine. Staff must be aware that laptops which have not been connected to the SYFR network for any period of time may not have most up-to-date protection.

15. Staff Absence

Subject to the details of absence of a member of staff to whom a laptop has been allocated, arrangements may be made for the member of staff covering for the absence to have access to that laptop.

16. Staff leaving SYFR

Staff leaving SYFR must return their laptop to ICT Section.

It is the responsibility of the member of staff leaving SYFR to ensure that all files have been copied to the server and/or suitable media before the laptop is returned.

Before a laptop is re-issued to a new member of staff, all files on the local hard drive will be deleted and any personal settings or additional hardware or software will be removed.

17. Internet/E-mail and Wireless Connectivity

Laptops used to connect to the Internet and access e-mail must be used in accordance with SYFR's Acceptable Use Policies on the Internet and E-mail. Particular attention should be paid to the provisions relating to access to unsuitable material and activities which may compromise network security.

Connection to Internet Services other than those provided by SYFR may only be configured using a broadband connection via a combined router/ADSL modem, which includes a built-in hardware firewall.

Technological developments in the area of cordless connectivity e.g. wireless protocols, Bluetooth and infrared have significantly increased the risks of unauthorised interception of a signal and of unauthenticated links being made to other devices.

Staff should not use wireless connectivity to connect to any networks outside SYFR unless they are authorised to do so.

ICT reserve the right to disable wireless facilities on a laptop if deemed necessary.

18. Personal Use

Limited personal use of laptops is permitted, subject to the restrictions contained in this or any other related policy. Any personal use of laptops is expected to be in the employee's own time and is not to interfere with the person's job responsibilities or the job responsibilities of other employees.

Staff are not permitted to attach personal equipment e.g. printers, cameras, scanners to a laptop without first contacting ICT Section. If permission is granted, drivers, software etc. will be installed by ICT.

Where personal equipment has been installed on a laptop, ICT will not be responsible for any hardware or software support relating to the personal equipment and reserve the right to uninstall if they consider it to be affecting the performance of the laptop.

19. Technical Support

Laptops in need of repair must be returned to ICT Section. Staff must not attempt to repair any hardware faults under any circumstances. Where available, a replacement may be issued to the staff member whilst the repairs

are being carried out. Staff will be asked to collect their laptop when ready and return the “pool” device if issued.

It should be noted that manufacturers’ warranties do not normally cover damage caused by misuse or neglect and do not cover replacement batteries.

20. Insurance

Laptops given to staff on loan are covered by SYFR insurance policy for use in SYFR. This policy also covers use of the laptop at home, travelling to and from SYFR and when the laptop is taken off-site for training or to meetings. The insurance policy covers accidental and malicious loss and damage.

21. Monitoring

Staff should be aware that the use of laptops, including the contents of local drives, is monitored in accordance with this policy.

SYFR reserves the right to audit correct usage at any time, and the individual may be held liable for illegally held software or material e.g. in breach of copyright legislation.