LAPTOP POLICY

Security

Laptops are an essential business tool, but their very portability makes them particularly vulnerable to physical damage or theft. Furthermore, the fact that they are often used outside of the Organisation's premises increases the threats from people who do not work for the Organisation and may not have its interests at heart.

Portable computers are especially vulnerable to physical damage or loss, and theft, either for resale (opportunistic thieves) or for the information they contain (industrial spies).

Do not forget that the impacts of such breaches include not just the replacement value of the hardware but also the value of any data on them, or accessible information through them. Information is a vital asset. The Organisation depends very heavily on our computer systems to provide complete and accurate business information when and where we need it. The impacts of unauthorised access to or modification of important and/or sensitive data can far outweigh the cost of the equipment itself.

The following guidelines must be observed:

1. The physical security of 'your' laptop is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert to the risks

2. Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop

3. If you have to leave the laptop temporarily unattended in the office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but deter casual thieves

4. Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. **Never** leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the boot or glove box but it is generally much safer to take it with you

5. Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Don't drop it or knock it about. Bubble-wrap packaging may be useful. An
ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag

6. Keep a note of the make, model, serial number and the Organisation's asset label of your laptop but do not keep this information with the laptop. If it is lost or stolen, notify the Police immediately and inform the *IT Manager* as soon as practicable (within hours not days)

7. Viruses are a major threat to the Organisation and laptops are particularly vulnerable if their antivirus software is not kept up to date. The antivirus software MUST be updated every time the laptop is switched on. If you are unsure on any points, contact the Internal IT Manager for advice on obtaining and installing antivirus updates

8. E-mail attachments are now the number one source of computer viruses. Avoid opening any e-mail attachment unless you were expecting to receive it from that person

9. Always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, e-mail attachments or files from the Internet). Virus scans normally happen automatically but the Internal IT Manager can tell you how to initiate manual scans if you wish to be certain

10. Report any security incidents (such as virus infections) promptly to the Internal IT Manager in order to minimise the damage

11. Respond immediately to any virus warning message on your computer, or if you suspect a virus (*e.g*. by unusual file activity) by contacting the Internal IT Manager. Do not forward any files or upload data onto the network if you suspect your PC might be infected

12. Be especially careful to virus-scan your system before you transmit any files outside of the Organisation. This includes E-MAIL attachments and CD-ROMs that you create

13. You must use password protection on all corporate laptops in accordance with the Organisation's Password Policy

14. You are *personally accountable* for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends or IT staff

15. Corporate laptops are provided for official use by authorised employees. Do not loan your laptop or allow it to be used by others such as family and friends

16. Avoid leaving your laptop unattended and logged on. Always shut down, log off or activate a password protected screensaver before walking away from the machine.

Unauthorised software

Do not download, install or use unauthorised software programs. Unauthorised software could introduce serious security vulnerabilities into the Organisation networks as well as affecting the working of your laptop. Software packages that permit the computer to be 'remote controlled' (*e.g*. PC anywhere) and 'hacking tools' (*e.g*. network sniffers and password crackers) are explicitly forbidden on Organisation equipment unless they have been explicitly pre-authorised by management for legitimate business purposes.

Unlicensed software

Be careful about software licences. Most software, unless it is specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and Organisation into disrepute by breaking the law.

Backups

Unlike desktop PCs which are backed up automatically by IT, you must take your own backups of data on your laptop on a regular basis – ideally daily but weekly at least. It is your responsibility to take regular offline backups to CD/DVD, USB memory sticks *etc*. **Make sure that offline backups are encrypted and physically secured.** Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop. Offline backups will save you a lot of heartache and extra work.

Laws, regulations and policies

You must comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example. Various corporate security policies apply to laptops, the data they contain, and network access (including use of the Internet).

Inappropriate materials

Be sensible. The Organisation will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or e-mail messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites. IT staff routinely monitor the network and systems for such materials and track use of the Internet: they will report serious/repeated offenders and any illegal materials directly to management, and disciplinary processes will be initiated. If you receive inappropriate material by e-mail or other means, delete it immediately. If you accidentally browse to an offensive website, click 'back' or close the window straight away. If you routinely receive a lot of spam, contact the Head of Operations (ISMS Manager) to check your spam settings.

Health and safety aspects of using laptops

Laptops normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury and balancing the laptop on your knees hardly helps the situation. Limit the amount of time you spend using your laptop. Whenever possible, place the laptop on a conventional desk or table and sit comfortably in an appropriate chair to use it. If you tend to use the laptop in an office most of the time, you are advised to use a 'docking station' with a full-sized keyboard, a normal mouse and a display permanently mounted at the correct height. Stop using the portable and consult Health and Safety for assistance if you experience symptoms such as wrist pain, eye strain or headaches that you think may be caused by the way you are using the portable.

Policy Sign-off

Date of Issue:	16/11/2020
Date of Next Review:	30/09/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	30/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Updates to responsibilities and date
3.0	16/11/2020	Jo Holloway	Job title update