

## **Information Technology Policy**

This policy provides guidance about acceptable use and security of IT resources including hardware, software and networks, provided by Riverside Training. This policy applies to all access relevant to the company whether this is on a computer/laptop company premises or mobile use of a laptop at home and use of the software through a home computer.

The policy establishes a framework and describes the standards that users are expected to observe when using these facilities and ensures that users are aware of the legal consequences attached to inappropriate use of the facilities.

This policy should be read in conjunction with other policies and procedures pertaining to acceptable standards of conduct and behaviour that can be found in the Staff Handbook and Health & Safety Policy.

This policy complies with the Regulation of Investigatory Powers Act 2000, Telecommunications (Lawful Business Practice) Interception of Communications) Regulations October 2000, the Human Rights Act 1998 and the Data Protection Act 1998.

This Policy will be monitored and reviewed on an annual basis by the Strategic Management Group.

## **Context**

All Riverside Training's IT facilities and information resources remain the property of Riverside Training. By following this policy, it will help to ensure IT facilities are used:

- legally;
- securely;
- without undermining Riverside Training;
- effectively;
- efficiently;
- consistently; and
- in a spirit of co-operation, trust and consideration for others;

The policy relates to all Information Technology facilities and services provided by Riverside Training. All staff and learners are expected to adhere to it.

## **Responsibilities**

- Riverside Training uses the services of a specialist IT Support who can be contacted through the Office Manager.
- Individual users should inform the Office Manager if IT equipment in their workspace fails to operate and the Office Manager will arrange for IT Support to be contacted.
- All mobile technology will be stored in a lockable cupboard which can be accessed through the Admin Team.
- Staff are responsible for the safe storage and operation of any mobile technology given to their care.

## **Precautionary and Disciplinary Measures**

Deliberate and serious breach of the policy statements will lead to disciplinary measures being taken as outlined in the Staff Handbook which may include the offender being denied access to computing facilities.

### **2.1 Copyright:**

All users should take reasonable care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

### **2.2 Security:**

Users should not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you don't have access to information resources you feel you need, contact your IT Support person or Office Manager for further guidance.

Users should not disclose personal system passwords or other security details to other staff, volunteers or external agents and must not use anyone else's login; this compromises the security of Riverside Training. If someone else gets to know your password, ensure you change it or inform the Office Manager to get IT Support to help you.

Any employee found to be accessing the company network and/or associated software packages with another employee's password without the authorisation of the Office Manager will be dismissed.

Disclosure of personal passwords to other staff, volunteers or external agents: This may be necessary in some circumstances. Such a practice is allowed only if sanctioned by a member of the Management Team after discussion with the IT Support. If the password is disclosed for a one-off task, the owner must ensure that his / her password is changed (by contacting IT Support) as soon as the task is completed.

If you leave your PC unattended without logging off, you are responsible for any misuse of it while you're away. It is the employee's responsibility to ensure that when not attended his/her system is suitably secured in order to prevent any fellow employees or third parties from accessing company information they are not authorised to view.

ALWAYS check disks for viruses, even if you think they are clean (contact IT Support to find out how). Computer viruses are capable of destroying Riverside Training's information resources. It is better to be safe than sorry.

Information about people: If you're recording or obtaining information about individuals make sure you are not breaking Data Protection legislation. This includes the user not sharing the information with third parties.

Users are advised to keep master copies of important data on Riverside Training's network and not solely on your PC's local C: drive or floppy discs. Otherwise, it will not be backed up and is therefore at risk.

### **3. Responsible use of Email**

When to use email:

Email should be used in preference to paper to reach people quickly and to help reduce paper use. It is advisable to check messages before sending (just as you would a letter or paper memo).

When circulating documents internally, it is recommended to refer to the documents location by a link to the shared drive rather than clog up email boxes and create unnecessary copies of the original document. Use Riverside Training's intranet to communicate all relatively static information (e.g. policy, procedures, briefing documents, reference material and other standing information). Use email merely as a pointer to draw attention to new and changed information on the intranet.

When publishing or transmitting information externally be aware that you are representing Riverside Training and could be seen as speaking on Riverside Training's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager.

Users should avoid using email where conflicts arise. An email can be easily misinterpreted; users are advised to speak to individuals directly if the content of an email may create confusion, misunderstanding or conflict.

Only send Emails to those it is meant for; don't broadcast to all staff unless absolutely necessary since this runs the risk of being disruptive. Unnecessary (or junk) email reduces computer performance and wastes disc space.

If you wish to broadcast other non-work related information or requests (e.g. information or opinions on matters outside the scope of Riverside Training's business activities, it is better to use a personal email account at home; not during work time.

Users should avoid broadcasting emails with attachments to large groups of people - either note in the email where it is located for recipients to look, or include the text in the body of the email. Failure to do this puts an unnecessary load on the network.

Users are advised to keep their inbox up to date, checking emails regularly and deleting, archiving emails as a matter of course. Keep electronic files of electronic correspondence, only keeping what you need to. Don't print it off and keep paper files unless absolutely necessary.

Don't forward emails warning about viruses (they are invariably hoaxes and IT Support will probably already be aware of genuine viruses - if in doubt, contact them for advice).

**Email etiquette:**

Being courteous is more likely to get you the response you want. Do address someone by name at the beginning of the message, especially if you are also copying another group of people. Make your subject headers clear and relevant to your reader(s) e.g. don't use subject headers like "stuff"

Capitals (e.g. NOW) can also be used to emphasise words, but should be used sparingly as it is commonly perceived as 'shouting'.

Treat others with respect and in a way, you would expect to be treated yourself (e.g. don't send unconstructive feedback, argue or invite colleagues to publicise their displeasure at the actions/decisions of a colleague).

Don't open an email unless you have a reasonably good expectation of what it contains,  
e.g. Do open report.doc from an Internet colleague you know Don't open explore.zip sent from an address you've never heard of, however tempting. Alert IT Support if you are sent anything like this unsolicited.

**Monitoring of emails**

The company regularly monitors all employees' email traffic; however, it is company policy not to view the content of any employee's emails unless:

During the monitoring process, it is identified that there is excessive email traffic to non-business-related contacts.

They form part of a formal disciplinary investigation.

Employees should be aware that if formal disciplinary action is being taken all emails (sent, received or deleted) might be accessed by the company. Emails will only be accessed if they are of direct relevance to the disciplinary matter being addressed, e.g. breach of confidentiality, harassment etc.

If during investigation it is found that an employee is misusing company email facilities formal disciplinary action will be taken that could result in dismissal.

Any employee found to be sending offensive emails either internally or externally will be dismissed.

**External data/programs**

Employees are not permitted to install any external data or software (including internet downloads) without the prior permission of the Office Manager. All software/data MUST be virus checked prior to installation. Any employee introducing data/software or downloading files from the Internet without authorisation may have formal disciplinary action taken against them.

**Internet Usage**

Internet access is provided by the company for business use. However, the company does appreciate that employees may wish to use company internet facilities for personal reasons.

The company has no objection to employees using company internet facilities as long as any non-business related activities do not breach the company's policies on computer/internet usage and are undertaken in the employee's own time.

Employees caught utilising the company computer and internet systems for personal usage in working time will have formal disciplinary action taken against them.

**Monitoring of internet use**

You are a representative of Riverside Training when you're on the Internet. Users should ensure their actions are in the interest (and spirit) of Riverside Training and do not leave Riverside Training open to legal action (e.g. libel).

The company regularly monitors all employees' internet access logs, however, it is company policy not to view the internet sites visited by employees unless:

- During the monitoring process, it is identified that there is excessive viewing of non-business related sites.
- During the monitoring process, it is identified that employees have been actively accessing pornographic or other unsuitable sites.
- It is brought to the company's attention that employees have been accessing Internet sites of a pornographic or offensive nature.
- They form part of a formal disciplinary investigation.

**Unsuitable Internet Sites**

The company is fully aware that during the normal course of an employee's daily duties he/she may on rare occasions be linked without his/her knowledge or intention to pornographic, offensive or otherwise unsuitable sites. If this situation occurs employees must exit the site immediately and notify the Office Manager that they have accessed a restricted site. Any employee found deliberately or repeatedly accessing sites of a pornographic, offensive or otherwise unsuitable nature will be dismissed.

Any employee found using company equipment to download or store pornographic, offensive or otherwise unsuitable material will be dismissed.

## Miscellaneous

Hardware and Software: All purchases should be approved by the Finance Manager, preferably through an identified IT budget.

Data transfer and storage on the network: Ask for advice from IT Support if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring your network to a standstill. Be considerate about storing personal (non-Riverside Training) files on Riverside Training's network.

## Care of equipment:

Don't re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.) without first contacting IT Support.

Don't take food or drink into rooms which contain specialist equipment like servers. Access to such rooms is limited to authorised staff.

## Environmental impact of IT

Riverside Training is committed to reducing the environmental impact of its services, wherever possible, and to this end has introduced a number of measures:

1. Automatic shutdown of computers when not in use,
2. Recycling of printer cartridges and waste printed output, and
3. Double-sided printing on the photocopier
4. Black and White photocopying will be set as default unless otherwise selected.

This policy will be reviewed on an annual basis.

<b>Current Review Date</b>	June 2023
<b>Next Review Date</b>	June 2024

IT Policy V1.3 June 23