Communications and Use of Equipment Policy

Statement of policy and purpose of policy

Floorskills (the **Employer**) provides staff with access to a range of communications and information technology equipment and systems (**Resources**) both as a shared resource in the workplace and also through individual allocation of items for use inside or outside the workplace. It is our aim and responsibility to:

- provide you with all the Resources necessary for the proper performance of your duties, in a reasonable and economical manner.
- ensure the security of Resources against unauthorised access or abuse whilst ensuring their accessibility to authorised and legitimate users.

The purpose of this document is to explain to staff the standards we require them to observe in using our Resources and the consequences of not adhering to these as well as to explain our policy in respect of monitoring use of our Resources.

This is a statement of policy only and does not form part of your contract of employment. We may amend this policy at any time, in our absolute discretion.

Who and what does this policy cover?

This policy and the rules contained in it apply to:

- All staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (Staff); and
- All use of our Resources including but not limited to use (and misuse) of computer servers and other hardware or equipment, desktop or portable computers, laptops and mobile telephones, smart phones, networks and systems, software, applications, subscriptions to databases and electronic resources, scanners, printers, memory or storage devices, copiers, CCTV, email, the internet and any data sent from, received by, or stored on our computer or communications equipment or systems.

The Managing Director has overall responsibility for this policy and has appointed himself as the person with day-to-day responsibility for the Employer's Resources.

All Staff have personal responsibility to use our Resources in a professional, ethical and lawful way and ensure compliance with this policy. You are expected to protect our Resources from unauthorised use or access at all times. Managers have special responsibility for leading by example and monitoring and enforcing compliance. Any breach of this policy will be taken seriously and may result in disciplinary action.

Personal use of Resources

Our Resources are provided to support Staff in the proper performance of their duties. You may not make any personal use of Resources.

Guidelines for PC and Laptop Use

Each employee has responsibility for the appropriate use and day-to-day care of their office

computer workstation and any computer equipment provided for use on or off our premises. You may not connect personal equipment or peripherals, for example, memory sticks, mp3 players or digital cameras, to our Resources unless this has been authorised in advance by the Managing Director.

You will log on your computer using an individual user name and password. You must not log on to any computer using someone else's name and password or otherwise use our Resources in a way that would lead us to believe that your activities are somebody else's, unless this has been approved in advance by the Managing Director even if you have the consent of the individual concerned.

Do not leave your computer accessible to others when you are not at your computer. Lock your screen or logout whenever you are away from your computer for more than a few minutes.

Using Resources outside work

If you are given authorisation to use any Resources away from our premises, including at home, (Remote Resources) then you must take appropriate care of the any equipment provided to use, ensure it is well-maintained and used in accordance with our rules, including this policy and with specific instructions given to you by the Managing Director. We may inspect Remote Resources without prior notice and, if asked, you must immediately return any equipment to us for inspection or maintenance.

Remote Resources provided to you are your responsibility. You must take reasonable steps to ensure the security of any equipment provided to you for use outside the workplace. If you are transporting equipment by car, it should be locked and left out of sight when the vehicle is unattended (eg in the boot of a car).

We provide equipment and other Resources for use outside the workplace in our absolute discretion and may withdraw this entitlement at any time. You must immediately return any Resources to us if we ask you to and, in any case, when your employment ends.

Email guidelines

Email is an efficient and cost-effective means of communication and we encourage its appropriate use for business related purposes. However, inappropriate or negligent use of email carries significant risks.

Your communications by email, like all other modes of communication, must not breach our disciplinary or workplace rules or any other policy and procedure and must not cause us to be in breach of obligations we owe to others. See the Misuse of Resources section of this policy, below, for further information.

Confidentiality is a particular concern when using email. You must be careful in addressing messages to make sure that communications are not inadvertently sent to unintended recipients. In addition, although we take steps to protect data security, you should be aware that the confidentiality of data (including email messages) sent via the internet cannot be assured. You should only send price sensitive or commercially sensitive information belonging to or relating to us with the prior authority of the Managing Director unless the emails and any attachments are password protected or encrypted in line with our guidelines.

Delivery of email cannot be guaranteed. If your email is urgent or important, check that it has

arrived safely with the intended recipient.
In general, you should not:

- distribute chain mail, junk mail, jokes or gossip, trivial or unnecessary messages; or.
- agree to terms, enter into contractual commitments or make representations by email unless you are authorised to do so.

If you are sent an email in error you should delete it and notify the sender. You should disclose or use any confidential information it contains.

Bear in mind that viruses may lurk in attachments or links sent by email. While we take measure to protect against viruses, do not open emails or attachments or click on links unless they are from a source that you know and trust. If you see any virus alert or notification on your computer, contact the Managing Director immediately.

In using email, you should observe the standards for communication that we expect for other forms of writing, including as to style, content and choice of language. Always consider whether there is a more suitable method of communication, for example, where there is a need to preserve confidentiality or in the case of sensitive issues which should be communicated face to face.

Do not use your work email address to register or sign up for online services or otherwise to communicate with any provider of goods or services, since this is likely to increase the amount of spam email that we receive as a business.

You must comply with any guidelines that we issue concerning filing, archiving and deletion of emails.

If you are out of the office on a working day you must create an automated "out of office" message to alert correspondents to your absence and the arrangements for dealing with any urgent queries.

All emails sent using our Resources must include the following disclaimer text:
Floorskills Training Centre is operated and run by Floorskills Limited, for the delivery of training courses, apprenticeships and NVQ qualifications within the floorcovering trade.
Please consider the environment before printing this e-mail
Visit our website floorskills.co.uk for information and advice on training, apprenticeships and on-site assessment.
Files attached to this email have been checked with virus detection software prior to transmission but you should still carry out your own virus check before opening any attachments. Floorskills Limited does not accept liability for any damage or loss which may be caused by software viruses.
The contents of this e-mail and any attachments are the property of Floorskills Limited and are intended for the use of the recipient only. If you have received this e-mail in error, please immediately notify us at info@floorskills.co.uk and delete it.
Floorskills Training Centre is operated and run by Floorskills Limited, registered in England - company number 08060930 .

Guidelines for Internet Use

When using the internet, remember that each website that you visit has the ability to detect information about you, including our identity as an organization and, potentially, your identity and who you are, and whom you represent. The information that you input on a website may be accessed by third parties, anywhere in the world. Accordingly, judgement and discretion should be used in determining the websites that you choose to access and your activities on that site.

You must read and comply with the terms and conditions of any website that you access using our Resources.

You must not:

- disable, alter settings on or interfere in any way with any measures implemented by us to ensure the security of Resources and/or avoid computer viruses in connection with internet use, including our firewall arrangements;
- visit any gambling, gaming, adult or other inappropriate website, including any website that is offensive, insulting, discriminatory or obscene or is likely to damage your reputation or our reputation;
- use illegal file sharing websites;
- download any program, data, game or other material from the internet except with the prior approval of the Managing Director, because of the prevalence of viruses on the internet.

Guidelines for Software Use

Most of the software and applications we use are licensed from third parties and our use is subject to terms and conditions. You must always comply with the terms of any software licence we hold. You must not copy, download or install any software or application except with the prior approval of the Managing Director.

If any computer, phone, Blackberry or other hardware we have provided to you prompts you to update or renew any software or application licensed to us, then you must do so promptly, unless we have told you not to. Only software or applications provided or authorized by the Managing Director may be installed on our Resources including but not limited to on your desk computer or laptop and any Remote Resources. You may not install other computer games, internet files, software, applications or other programmes on our Resources.

Monitoring of use of our Resources

We may monitor and intercept your use of our Resources, including your internet use and communications sent to you or received by you, by phone, email (including associated files or attachments), fax or any other means, involving our Resources for a number of relevant business reasons, including but not limited to:

- ensuring compliance with the terms of this policy.
- training and monitoring standards of service.
- ensuring compliance with regulatory practices or procedures imposed or recommended by any regulatory body relevant to our business.
- ascertaining whether internal or external communications are relevant to our business.
- preventing, investigating or detecting unauthorised use of our IT systems or criminal activities.
- maintaining the effective operation of our Resources - in particular, all emails received by the Employer are automatically scanned for viruses.
- establishing the existence of facts.

Since you are not permitted to use our Resources for personal use, you should not have any expectation of privacy in respect of your use of our Resources, including with regards to communications sent to you or received by you, by phone, email (including associated files or attachments), fax or any other means.

Certain authorised employees involved in administering our Resources may necessarily have access

to the contents of email messages in the course of their duties. Any knowledge thus obtained should not be communicated to others, unless necessary for legitimate business reasons.
We may also take any action in administering email or other communications that is reasonably necessary to preserve the integrity or functionality of our Resources including as part of a firewall or spam or virus protection arrangements. This could include the deletion or non-transmission of any emails or communications (including any personal communications).

You should note that a CCTV system monitors all workshop, training areas and warehouse facilities 24 hours a day and this data is recorded.

Password policy

Appropriate passwords are vital to maintaining the security of our Resources.
In general, to access certain Resources such as computers, mobile phones or other devices or certain information sources or accounts, it will be necessary to enter a password or personal identification code. Passwords should be kept private and are the direct responsibility of the person to whom the account or device is allocated. Where access to any device or equipment that we provide to you can be secured by a password or code, you must use that facility.

Password standards

Passwords used on our Resources should adhere to the following standards, where permitted by the device or account in question:

- they must contain at least 8 characters in total and at least one of each of the following:
- numeric character
- they should not be a dictionary word in any language, slang, dialect, jargon, etc.
- they should not be based on readily available information about you like your date of birth, spouse's or child's name, telephone numbers or address.
- they should not be the same as or contain your name or username.
- you must not use the same password on our Resources as you do for your personal accounts or devices.
- they must differ materially from previous passwords.

Password security

You are personally responsible for maintaining the security of your passwords used on our Resources. You must not disclose your password to anyone else, inside or outside the Employer, except as directed by the Managing Director. You may not keep a written record of your passwords anywhere on our premises or any device unless it has been encrypted.

You must not attempt to access any restricted area of our Resources or to guess or determine the password of any other user.

You must change your main computer log in password when prompted to do so either automatically or by the Managing Director.

If you become aware or suspect that your password has become known to another person then you must immediately change it and notify the Managing Director of the situation.

On termination of your employment, however arising, or if requested to do so by the Managing

Director, you must provide details of all passwords used on our Resources to the Managing Director.

Misuse of Resources

The same principles apply to your use of Resources for communication including through email, telephone and the internet as apply to any means of communication and you must not use these for any purpose or in any way which could be subject to disciplinary or legal action in any other context.

In particular, you must not use our Resources in any way that:

- breaches obligations of confidentiality which you owe to us or to any third party or which causes us to breach duties of confidence which we owe to any third party.
- breaches the rights of any other Staff member to privacy, data protection and confidentiality or which amounts to bullying or harassment.
- is offensive, insulting, immoral, discriminatory, obscene, pornographic or sexually explicit.
- poses a threat to our confidential information and intellectual property.
- infringes the intellectual property rights of any other person or entity.
- defames or disparages us or our associated companies or to any party with whom we have a business relationship, such as suppliers or customers.
- breaches or causes us to breach any law or the rules or guidelines of any regulatory authority relevant to our business.
- breaches data protection rules.
- breaches our rules, policies or procedures for the use of our IT Systems or other equipment or resources.
- is dishonest, improper, unethical or deceptive (eg pretending to be someone or attempting to access another employee's computer, computer account, email, files, or other data);
- is likely to damage your reputation or our reputation.
- wastes Resources or use them excessively or to the exclusion of others.
- interferes with the work of others or our computer, technology or communications systems.

Further, you must not:

- delete, destroy or attempt to modify our Resources or any information contained on them except in line with this policy or instructions given to you by the Managing Director;
- use our resources to conduct any business other than our business.
- You should also note that the following activities are criminal offences:
- unauthorised access to computer material (hacking); and
- unauthorised modification of computer material.

Fire Walls

51. **Firewall Protection:**

Huawei Firewall (Router)
Stateful Packet Inspection (SPI) is enabled.
Inbound (from Internet to LAN) policy: Dropped.
Remote authorized access will override the inbound policy.
Outbound (from LAN to Internet) policy

52. **Filtering strategy set up to monitor and protect:**

MAC filtering:
Whitelist and blacklist
IP filtering:
Whitelist and blacklist

URL filtering:
Whitelist and blacklist
DOS attack

53. **Microsoft Pc's:**
Windows network firewall active
AVG Antivirus

54. **Anti-virus:**
AVG anti-virus on older PC's
Windows security on newer windows 10 Pc's
Other relevant policies
55. Staff are referred to the Staff Handbook for other policies and procedures which may be relevant to the issues covered in this policy.