IT ACCEPTABLE USE POLICY

(Employers & Learners)

Person Responsible	Date Reviewed
Andrea Keeley	5/1/2021

PURPOSE

The purpose of this document is to bring into line Profile's IT and password policies in line with Cyber Essentials. All staff must read this, understand how it affects them and must adhere to this policy at all times.

This policy covers the use of:

- Any IT Equipment (including but not limited to Desktop PCs, laptop PCs, tablets)
- Information Systems and Applications (whether or not networked)
- The Internet and Intranet
- Email (both internal and external)
- Portable Data storage devices (including but not limited to external hard drives, memory sticks etc)
- All telephone systems and services, including mobile phones.

OVERVIEW OF POLICY

Information technology (IT) equipment, information systems, electronic communications systems and data are essential tools for conducting business in todays society. Profile supplied equipment is only to be used for the purpose for which they have been provided, and may be withdrawn by Profile if used inappropriately. Misuse of any such system or data and the possible consequences of such misuse, may result in disciplinary proceedings, potentially resulting in dismissal and criminal prosecution.

PASSWORDS

You must not disclose your password to anyone, including your manager or anyone else who asks for it. It is your responsibility to keep it secure. If another person becomes aware of your password you must change it immediately and report the matter to your line manager. Passwords must be changed regularly and some systesms automatically prompt you to do this. Passwords must be a minimum of 8 characters, including at least one capital letter and one number.

You must also:

- Avoid choosing obvious passwords, such as those based on easily discoverable information like the name of your favourite pet
- Do not use the same password anywhere else, at home or at work
- Passwords may be stored electronically, such as in a password vault or password manager, which is appropriately secured. This could be Google Password Manager, when 2 factor authentication is required for example. If you are unsure which method to use, please speak to your line manager.

DATA CONFIDENTIALITY

All data held on Profile's IT systems must be safeguarded at all times, in line with the contents of this policy and the Privacy GDPR policy.

Working for a company does not give you the automatic right to have access to, or gain knowledge of, all data that is held by that company. You are entitled to access only the data that

- you are authorised to do so
- have a clear, unambiguous, proper and legitimate business need to do so
- be solely for the purposes of performing the duties of your job, or
- are directed to access by one of the Directors or Senior Management of the company.

You must not copy, amend, delete or remove any information held by Profile unless you have a clear business need to do so.

You must not send or communicate any such information to anyone outside of Profile unless you are specifically and legally permitted to do so. Unauthorised disclosure of this kind may be subject to disciplinary action up to and including dismissal and possible criminal prosecution.

This also means that you must not:

- Trace customer information for entertainment, personal or casual interests
- Reveal information obtained from documents to any colleague unless there are business reasons to do so
- Access a document
    - For curiosity
    - For any personal non business-related reason
    - Where there could be any conflict of interest

The principles of access to and confidentiality of customer records apply equally to other records and information held on IT equipment, including information about colleagues.

You should be in no doubt that employers take a very serious view of any breaches of customer confidentiality. To protect their reputation and the interests of its customers, it is expected that employers will treat <u>any</u> breach of the confidentiality rules and obligations as potential <u>gross misconduct</u>, and, as such, would be likely to lead to dismissal, if proven.

It is fundamentally important that data relating to Profile's customers is kept secure and that the customers have confidence that their records will not be subject to unauthorised access or risk being disclosed.

ACCEPTABLE USE

To explain what is acceptable, it is simplest to describe what is NOT ACCEPTABLE. In general, it is essential that you do not do anything which is:

- Illegal
- Likely to cause embarrassment, annoyance or offence to other people
- Against Profile's values, specific guidance or expected standards of behaviour
- Likely to have negative consequences on the reputation of Profile
- Likely to result in a loss of data or productivity

This means that you must not access, view, create, use, store, download, install, distribute or circulate any material including images, text or software that:-

- Is or might be considered violent, indecent or obscene e.g. pornography
- Is or might be considered to be offensive, abusive, could be taken as a personal attack, or is rude, sexist, racist or generally distasteful
- Wastes time or IT resources, for example forwarding chain mail or jokes
- Encourages or promotes any unlawful activity or incites criminal behaviour
- Has the potential to damage or overload networks, systems or communications channels eg. downloading of software or other computer programmes
- Might be defamatory or adversely affect the company's/organisations reputation or image
- Might encourage a fundamental breakdown in relations or promote industrial action.

In addition, you must not promote any outside business or cause, financially or otherwise, and whether commercial, political, cultural or religious.

PERSONAL USE

A reasonable level of personal use of IT facilities is permitted **provided that this is in your own time**, will have no detrimental impact on your Company's/organisations business **and does not contravene this Acceptable Use Policy**. This facility is a privilege, not a right, and will be withdrawn in cases of abuse. Any personal messages you send must clearly be identified as such and clearly state that the message is not being sent on behalf of your employer. Any costs associated with the personal use of the employer's equipment or systems (for example the personal use of mobile phones) must be repaid.

LEGISLATION

All staff have an obligation and legal liability to assist Profile in complying with its responsibilities under all appropriate legislation, including the Data Protection Act 2018 and you must exercise due care when holding, processing or disclosing any personal data.

CARE OF IT EQUIPMENT

It is expected that staff take reasonable precautions to maintain equipment and any issues are reported immediate. Where staff use personal equipment for work use, such as mobile phones, operating and security systems must be kept up to date. If, or when, a personal electronic device no longer updates to the current system, the convenience of using your own device will be revoked and you will be provided with a compliant work alternative.