IT ACCEPTABLE USE POLICY

(Employers & Learners)

Person Responsible	Date Reviewed
Andrea Keeley	27/10/2022
Ian Pearce	01/04/2024

Contents

PURPOSE

The purpose of this document is to bring 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 Profile supplied equipment is only to be used for the purpose for which they have been provided, and may be withdrawn by Profile if used inappropriately.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 where online systems automatically prompt you to do this. Passwords must be a minimum of 12 characters or more. The National Cyber Security Centre recommends 3 random words which you can remember, but which do not naturally go together including special characters (*£%£!)

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.

Another layer of security to your password is to use 2 factor authentication (2FA) or multi-factor authentication (MFA). This process involves using your fingerprint, retina scan or a code being sent to a separate device such as your mobile phone to further verfity your identity. You should use 2FA or MFA where possible (see Appendix 1).

Your password must be changed immediately if you suspect it has been compromised your line manager and the Centre Administrator must be informed.

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.

To protect Profile's 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

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.

You must have anti-malware installed on your work devices. Laptops are administered by our IT Support company who ensure that this is up to date. Mobile phones must also have anti-malware installed, such as Norton 360 Antivirus and Security.

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 Profile's 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 immediately. 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.

Appendix 1

Password Creation

Passwords are important. Just think for a minute of your front door key. How many different doors does this key open? Would you be happy using a universal key to get into your house? Passwords are just like that unique key, they are an effective way of identifying and authenticating who you are. It is the first and sometimes the only layer that stands between you accessing your money, data, social media accounts and email or someone else accessing those assets and possibly compromising them, stealing from you, or locking you out.

The most common passwords still are, password, password1 and 12345678. Even a password of 8 characters can be cracked in about 5 hours using a standard office computer, and many passwords that are made up of dates of birth, names of your pets and children, your favourite band or football team can be easily worked out by reading your social media pages or googling you.

One password – one account

One of the biggest human-factor risks to businesses is staff re-using their passwords. If your work account access password is the same as your Facebook password, potentially a Facebook breach (or any of the other accounts where you use that username-password combination) could equal a big security problem for your organisation.

When an online company is breached, thousands of pieces of customer information can be stolen, including email addresses and passwords. The cyber criminals will immediately go through as many accounts (e.g. utility companies, eBay, Instagram, amazon, Hotmail, insurance companies) as they can, trying those user-name-password combinations hoping to open up an access point for more crime. This is the reason you need a separate password for each online account.

Your email address is the gateway for all your other accounts and the place where you reset your passwords. With this in mind, if a criminal gets access to your email account, they can take control of most other user accounts that you have. At the very least, have a complex and unique password for your email account that no one could guess. Password length and complexity attribute how much time it can take to crack the password by a cyber criminal.

Cyber criminals can use computers to guess people's passwords and break into their computers in what is called a Brute-force attack. The computer will try every combination of letter, literally working through the dictionary till they have found the words that work. Some programs are sophisticated enough to search logical substitutions such as '4' for an 'A' , 'I' for '1' etc. For this reason, it is recommended that you use a password that is over 8 characters long, or better still, 12 characters or more, make it complex and hard to guess, and if available you should lockout your accounts after a certain number of unsuccessful login attempts.

How do you think up a unique secure password for each of your user accounts and also remember them?

How to make a strong password

The National Cyber Security Centre has a great deal of useful advice about passwords. They recommend that you use three random words which you can remember but do not naturally go together. It is also a good idea to use numbers and special characters (*&%F£) in your password as well as a combination of upper and lower case letters. The longer your password the better. It is recommended selecting long passwords for your admin and other crucial systems' accounts (i.e. email account, banking account). Do not share your password with anyone, this is private information.

Looking after your passwords

The good news is that you do not need to remember all those long and complex passwords. You can use a piece of software called a Password Manager. You may have noticed that your browser already asks you if you'd like it to create and store passwords for you. This is a browser integrated Password Manager and is safe to use for personal use, however there are security issues linked to this kind of password manager.

It is recommended you use an independent, stand-alone password manager such as Last Pass or Dashlane. Do research third party password managers and use the one you feel is the safest. It is often as simple as downloading their software from their website and signing-up with your email address. You will then only need to remember one really good complex password to the Password Manager itself and after that, the Password Manager will remember your user names and create and remember extremely secure passwords for each of your accounts. It will be able to operate across multiple devices and on different browsers, it can also be asked to remember additional information such as addresses, wifi codes, credit cards, passports; all organised and encrypted. Password managers provide an option to configure multi-factor authentication to provide another layer of security.

Another layer of security

Another great way to add a layer of security to your password is to use 2 factor authentication (2FA) or multi-factor authentication (MFA). This process is being used more and more and involves using your finger print, retina scan, or a code being sent to a separate device eg your mobile phone to further verify your identity. If you have the option for 2FA or MFA*, use it where possible.

About 2 factor authentication

Two-factor authentication, or 2FA as it's commonly abbreviated to, adds an extra step to your basic log-in procedure for one of your online accounts. Without 2FA, you enter in your username and password, and then you're done. The password is your single factor of authentication. The second factor makes your account more secure. Multi factor authentication (MFA) is any number of factors more than one.

2FA or MFA requires the user to have two or more types of credentials before being able to access an account. Using two of the same type of authentication is not two factor.

The three types are:

- Something you know, such as a personal identification number (PIN), password or a security question (what is the name of your first pet?)
- Something you have, such as an ATM card, phone, or key fob (a small security device with built-in authentication)
- Something you are, such as a fingerprint, retinal pattern, or voice print. These factors are called biometrics.

Why is two factor authentication important?
Passwords have been the mainstream form of authentication since the earliest days of computing, however, if we consider that 90% of passwords can be cracked in less than six hours and two-thirds of people still use the same password everywhere, they may not be as secure as they need to be.

The vulnerability of passwords is the main reason for requiring and using 2FA. Implementing multifactor authentication will prevent hackers from gaining access to your accounts even if your password is guessed or stolen. The extra layer of protection that MFA offers ensures your account is more secure and drastically reduces the chances of fraud, data loss or identity theft.

What are the different ways to implement multi factor authentication?
The methods described below all involve 'something you have' methods of authentication. There is usually an enrolment process where the user logs onto a website or app with a username and password and follows a process to enable two factor authentication. Then for subsequent log ins, the process will ask for the second layer of authentication.

Time-based One-Time Password (TOTP)

TOTP involves the generation of a one-time passcode from a shared secret key. This can be generated by a physical device that the user is given such as key fob, a USB dongle or smart card which dynamically generates a token for the user. The code is valid for only a short time, sometimes as low as 30 seconds and is single use.
Alternatively, a user can download and install an application that runs on their computer or mobile device that dynamically generates tokens for the user. Software tokens work similarly to hardware tokens in that they are randomly generated and last a brief period of time before changing.

Short Message Service (SMS)
Perhaps the most common method of implementing 2FA. This method sends the user a unique token via SMS text message, normally a 5-10 digit code. The user then needs to provide this unique token before they are granted access.

Push notifications
Typically, push notifications work with applications. A push notification is sent to the app on your mobile device. This notification is a login request and includes information such as the application name, the Operating System and internet browser you are using as well as the location and the date of the request. The user accepts the request & automatically the user becomes logged in.

2FA codes can also be received via email and phone call. Regardless of the nature of the second layer, it serves as a vital barrier to your account.

Biometric authentication
Biometrics or 'something you are' authentication is considered the most secure and hardest to compromise form of 2FA. It's also more convenient, as users are the token, so the login process is quick and easy and they are not required to have their mobile device on them at all times. Physical identifiers can be fingerprints, facial features, iris or retina patterns or voice. Behavioural identifiers can be hand-writing analysis or typing patterns.

Biometric authentication, however, presents a number of issues related to storage of biometric data and privacy concerns. If your fingerprint or other biometric data is compromised, how do you change or reset it?

Can 2FA be breached?
While two-factor authentication does improve security, no security system is 100% safe.

The longer a 'new' security measure has been in place, the better the hackers get at breaking it. Using 2FA offers another layer of security and will definitely make an attack harder. This will discourage a large percentage of cyber criminals and give you a lot more security than just using a password. We should all strive to use 2FA wherever and whenever possible.

How to enable two factor authentication.
Most of your common accounts such as Google, Microsoft, Yahoo, Facebook, Linkedin, Twitter and Instagram have 2FA available for your log in. Simply enable it. Go to the security page in settings, click 2 factor authentication and then the get started button to sign in to your account and turn on 2FA.

Cyber Aware on the National Cyber Security Centre website has some great advice on how to switch 2FA on for your main accounts.

Backup option
If you are currently receiving 2FA codes via SMS, it is recommended that you set up at least one backup option in case you can't access your phone. You can print out a handful of backup codes that you'll then store in a safe place. You can also use Google Authenticator app as a backup option or USB security key.