# Protecting Our Borough's Information & Data

Our residents, customers and service users are our top priority, and we must at all times protect their information when delivering our services. To help do this we have taken additional measures to secure our systems and data. These measures include Multi-Factor Authentication (MFA) which requires Council IT system users to verify their identity using additional factors alongside their usernames and passwords). Verification is often completed by providing a text-code, a pin code or by using a smart phone authenticator app.

Almost all online services including banks, social media, and shopping secure your personal information in this way.

## What does this mean for me?

If you are a new employee, you will be asked to register for MFA on day-one of your employment if you will be accessing Council IT systems at home or work and/or have access to work emails on a personal device.

You will be asked to bring along your mobile phone/device on your first day at work and to provide contact details to register for MFA. This can be done by providing us with your mobile number to receive text-codes, or by choosing to receive notifications via the Microsoft Authenticator app which you can install on your personal device. This information is only used to verify your identity.

To access our IT systems you will be regularly asked to verify your identity via our chosen method i.e. text-code or via the App.

To find out more about Multi-Factor Authentication, watch this helpful introductory video

## Why is the Council using Multi-Factor Authentication?

Cyber-attacks on organisations' systems are becoming increasingly common and can have a very significant impact on both organisations and individuals. A cyber security incident can result in the loss of personal information about Council staff, residents and customers. It can also lock users out of Council systems and resources and disable key operations.

Successful cyber-attacks very often start through use of a compromised email or system account, where the attacker is able to log into the system using the account details of an authorised user. MFA is intended to make that much more difficult.

## How is my Multi-Factor Authentication device/contact information held by the Council?

Your device information and/or contact number will always be kept securely within North Tyneside Council's Microsoft 365 system. The information will only be used to verify your identity to log-in to Council systems and devices. Full details about how your information is stored, retained, and removed is available within the Council's Employee Privacy Notice on the Council's website.

## I have a question

Email your question to MFAhelp@northtyneside.gov.uk