

Welcome

Kirklees Council uses technology to work smarter.

We currently use

- Office 365 – Microsoft suite of applications and email in the cloud
- Outlook – emails/calendar
- Skype for business – which is an office communication system for messaging/calls and videoconferencing

All of this helps us to work smarter because they all interoperate and talk to each other seamlessly. This means you will be able to tell at a glance who is available, who is busy, their location and when they will be free to talk - even if they are working at home or in another office.

This pack gives some basic guidance on the Office packages and email system, along with information about keeping your reporting loss or theft of equipment and the support available to you through your Group Support & Development Officer, the Councillor Support Team and IT.

- 1 Details regarding Support
- 2 Instructions for authentication
- 3 Skype user guide
- 4 What to do in the event of loss or theft
- 5 Password/Equipment Guidance
- 6 Information Security Policy
- 7 Electronic Communications Policy
- 8 Removable Media Policy
- 9 Updating Multi-Factor Authentication details for Office 365

Member IT Help and Support

How to get help if something has gone wrong

IT Services are available at any time through an on-line portal where requests and issues can be logged and self-help guidance can be found. <http://itservicedesk/home>

A full support service will be operated through the IT Service Desk. Hours of support are:
07:15 – 17:30 Monday to Friday. This can be accessed through dialling internally using **ITServiceDesk** or **46883**, or externally on **01484 414728**. Your call will be answered and logged by our dedicated Service Desk team and attended to by a member of the team.

Alternatively you can email the IT Service Desk, at EB.ServiceDesk@kirklees.gov.uk

In addition to this IT will have a presence within Civic Centre 3, both with the Executive office and Councillor Support. This will be Monday to Friday 9 while 3, Councillor Support then have a direct route in to IT if there is anything urgent.

Limited support service is available (excluding bank holidays):

06:00 – 07:15 Monday to Friday

17:30 – 22:30 Monday to Friday

07:00 – 19:00 Saturday and Sunday

The numbers for calling this service are the same as for the full support service. This limited support service will offer targeted support dealing with a quick response to the most common IT issues such as password or system resets.

During the limited support hours your call will be answered by a colleague in our Support team who are usually working from home during these times. The majority of calls we have received from you have been around accessing your system, things such as password resets, these can generally be dealt with remotely and immediately and in most cases can be resolved during this first phone call. More complex issues may require access to the full range of technical skills and therefore may take longer. Our Support colleagues will answer your call personally if they can but if they are busy and cannot get to your call in time please leave a message and you will receive a prompt call back – usually within 30 minutes. You can also leave a message on the automated system for us outside of these extended times and we will contact you when we are next available.

Where to direct more general queries to ensure you get the best response

Some of the calls you raise are for advice or queries. Your councillor support team work closely with a dedicated IT Officers within Civic Centre 3. They understand the types of problems you face and what would best help you. A direct call during normal office hours to councillor support should be your first port of call. They will contact the IT team on your behalf if necessary. Taking this route will ensure you get your general queries and advice requests answered quickly and importantly you'll always be talking to someone who can offer you the best tailored advice. **Councillor support** can be contacted on: **01484 221000**. Of course you can continue to log these through the normal support numbers if you prefer.

What will happen if your issue is complex or can't be fixed remotely

On some occasions the issues you raise are complex or hardware related and unable to be dealt with remotely. In these cases we will arrange with you to bring equipment in or do our best to arrange for a site visit during normal working hours as long as it is planned with a least 48 hours' notice, although outside of this we will try to accommodate urgent requests. In an emergency we will transport staff to the job by whatever means required. In these more difficult situations these calls will be escalated to the Operational Manager and the Principal Officers in Support. They will manage these issues directly

Member IT Help and Support

with you through to resolution, keeping member support colleagues informed, and will work with you to agree the best course of action. During normal office hours, these people can be contacted on **01484 221000**.


Web Access and VPN logons using Two Factor Authentication

You will need a token to complete the two-factor authentication process. This is only required for VPN access to the Council Network and for use with Outlook Web Access.

If you do not already have a token, please contact the IT Service Desk (01484 221000 or email it.servicedesk@kirklees.gov.uk) and they will send one on to you.



You should hold the token with the button to the right hand side. When you press the button, a 6-digit number is provided which should be entered after the password as detailed below



Authorised Users Only
Kirklees Council Gateway

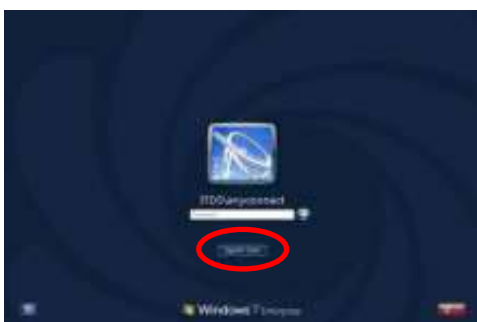
Username	<input type="text"/>	Please sign in to begin your secure session.
Password	<input type="password"/>	NOTE: Please use your Password & Token Number (with no spaces) in the Password & Token No field.
Password & Token No	<input type="text" value="<Password><Token No>"/>	If you have problems logging in, please call 01484 221000 and ask for IT Service Desk.

VPN Connections to the Council Network

Two factor authentication to the VPN logon process from PCs and laptops running Windows 7.



Press CTRL+ALT+DEL at the initial screen (if prompted).



Click on 'switch user' when prompted for password.



Then click on the additional 'network logon' icon in the bottom right hand corner of your screen

Click on this to launch anyconnect software.



Click on 'connect'



Enter your username, and password and token number details when prompted.

Accept the KMC Network policy. You will then see your normal login screen. Enter your password as normal and you should be on the network.

As before, the password should be entered on the following line, immediately followed by the code on the token.

Lync User Guide

Please check the Intranet for several guidance documents that are available.

In this guide:

- Using Skype
- Presence
- Instant Messaging
- Making a call
- Receiving a call
- Missed calls
- Voice Mail messages
- Voice Mail messages
- Things to know

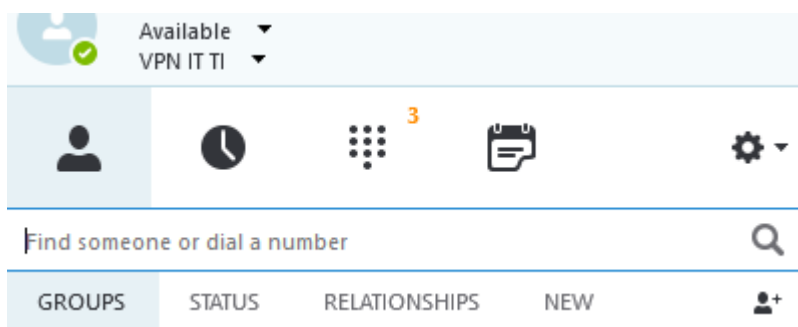
Using Skype

Once you have logged in you will see the Skype icon appear on your bottom bar

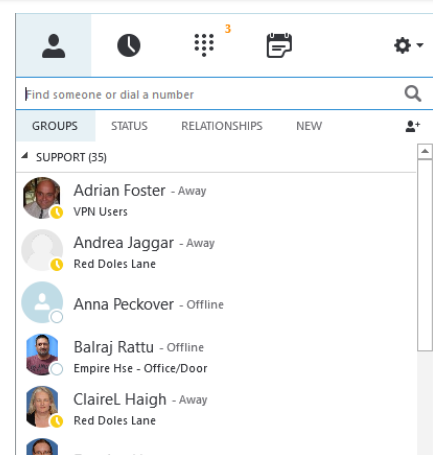


Click on the Skype Icon and the following screen will appear. At the top of this screen you will see four icons, these are:

1. Contacts
2. History
3. Phone
4. Phone



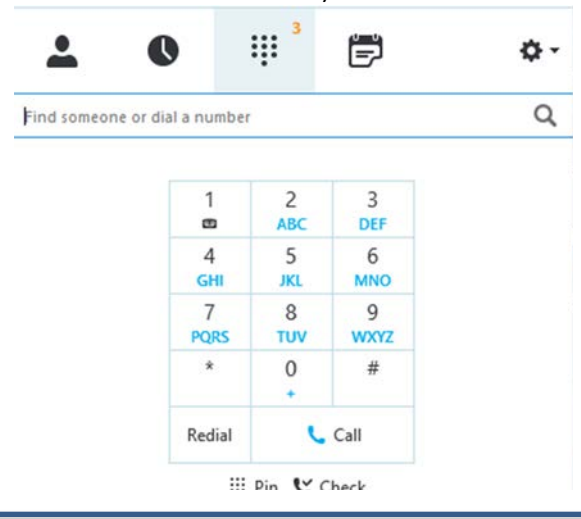
1 – Contacts – The **Contacts** tab will show you the Colleagues you are in contact with. You can choose to save new contacts in this section, and organise them into groups and/or teams if you so wish.



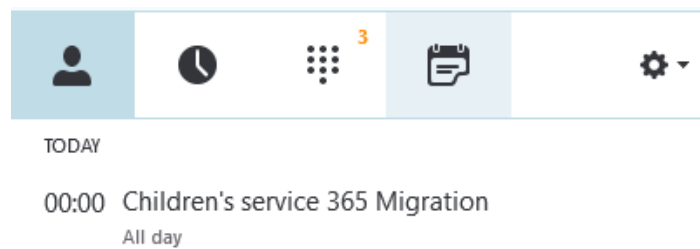
2 - History - The **History** tab will show you the missed calls and conversations. It will show the current status of the contact alongside the name as well.



3 - Phone - The **Phone** tab will enable you dial both internal and external numbers. (Note – external numbers always require you to dial the area code first.)



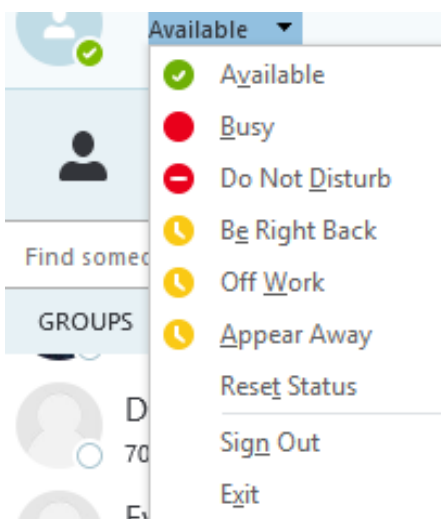
4 - Phone - The **Phone** tab will enable you dial both internal and external numbers. (Note – external numbers always require you to dial the area code first.)



Presence

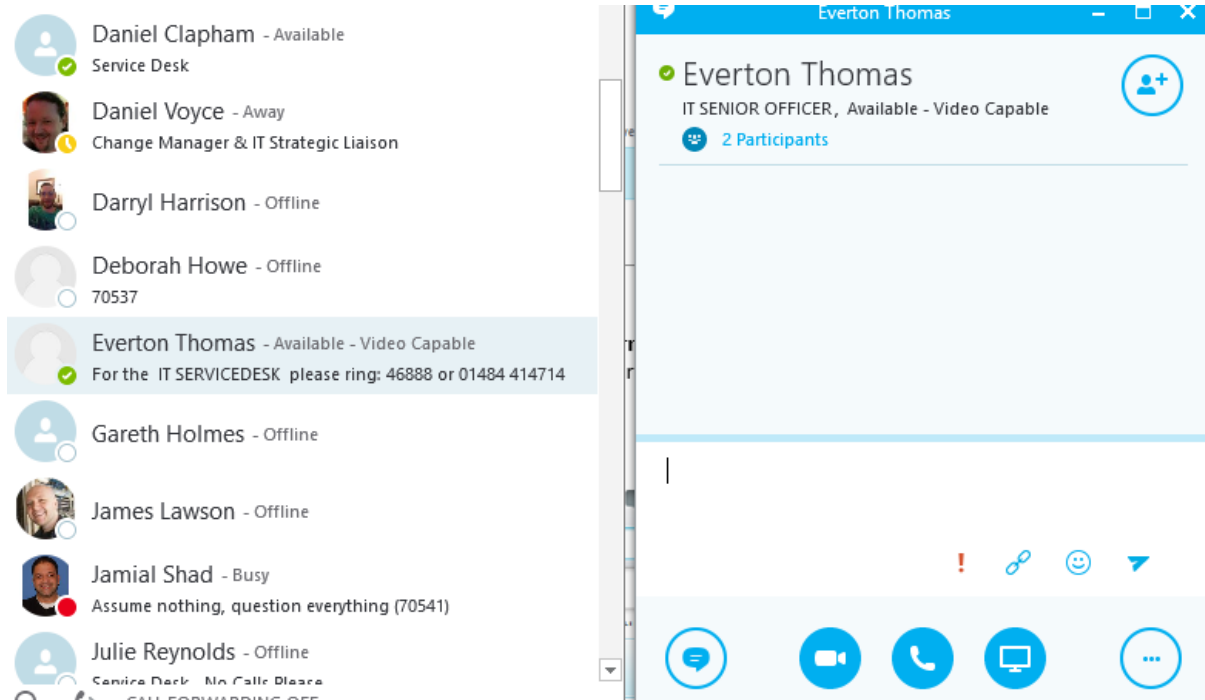
Skype provides an immediate, visual representation of a contact's availability, or presence. By simply looking at the contact list, you can find everything you need at a glance.

You can easily change your 'Presence' by left clicking on the tab under your name. Select the 'Presence' that is appropriate for you.



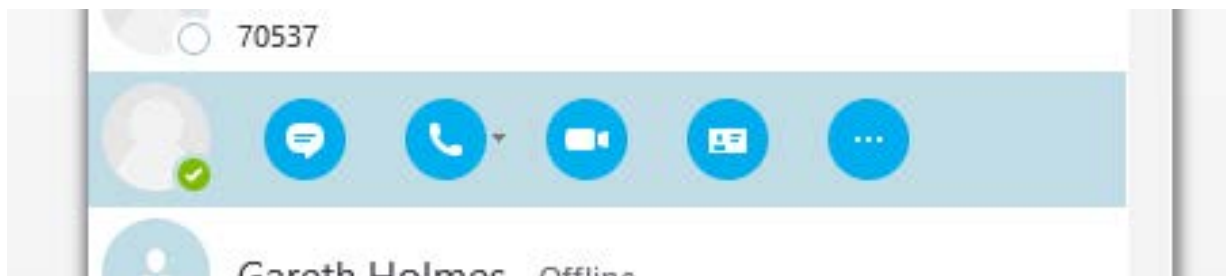
Instant Messaging

To send an instant message, double click on the contacts you wish to message. Alternatively, search for their name in the 'Find a Contact' box at the top of the Skype window. A new window will appear that will allow you to type a message to that person.



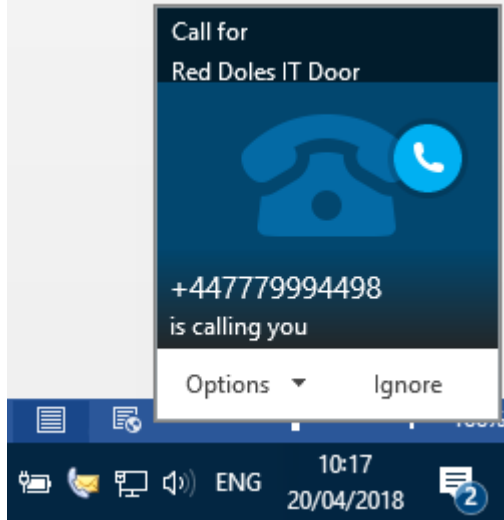
Making a call

You can use the phone section to dial the number you wish to ring. Please note **external numbers always need the area code dialling first**. You can also search for or select any of your contacts to call by selecting their name and then selecting the call tab. You can select the individuals picture of bubble and access the extra menu to call, message or video call them.



Receiving a call

When receiving a call in Skype the following box will appear:

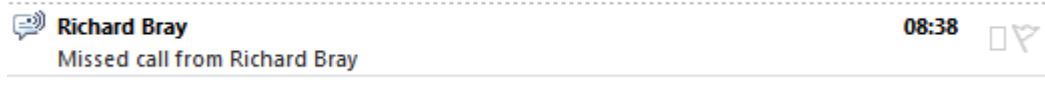


You can accept the call by pressing the green phone icon, redirect it to another person or your voicemail, or decline the call completely.

Please note that the presence and picture of the person calling you may not always appear. When a 3rd party company phones you, their number maybe the only thing that appears in the window. The same options will be there for you to make regarding the call.

Missed calls

Today



An email will appear in your inbox to say who has tried to contact you and when they have tried to contact you.

When you open the email you will get more details of the person / company who have tried to contact you.

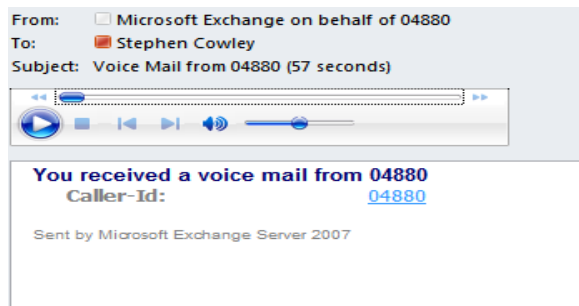


Voice Mail messages

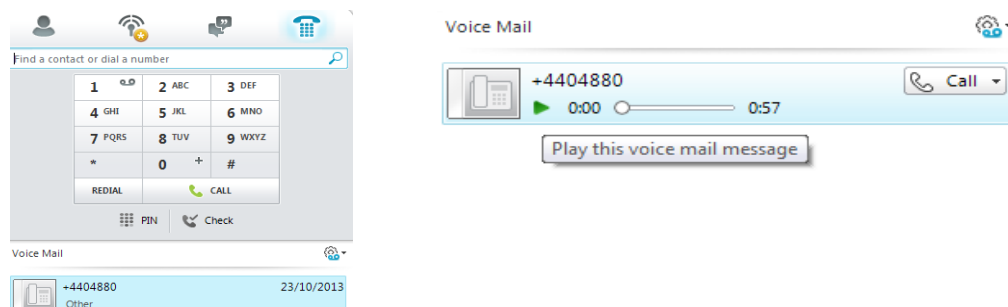
You will receive a Voice Mail message via an email in Outlook or you can view your messages in Lync.



The contents of the email will appear as below. To listen to the message select the play button.



Alternatively, select the Skype phone icon and choose the Voice Mail you wish to listen to from the Voice Mail list. Listen to the Voice Mail by selecting the play tab.



Things to know

Phone numbers

The extension number you have and the external direct dial number are both part of the telephone system we are replacing. Everyone will be given a new 5 digit number to use internally; external calls will come via the automated switchboard.

Making external calls

As your Skype phone travels with you wherever you log in, we can't tie it to a specific geographical location, such as Huddersfield or Dewsbury, so when dialling any external number you need to use the area code. You no longer need to dial 9 for an outside line just enter the phone number, including area code it into the search bar.

Updating people finder

Open People finder by clicking here, and on the right hand side there is a button called 'Edit my Profile'. This opens up your on profile, to edit any of the different sections click the Edit button in the top right hand corner of the section. To change your telephone number, click the edit button to the right of your name.

Switchboard problems

Please contact IT Helpdesk on 01484 414714 or 860 46888. This is the same number for any IT or Skype related issues.

Voicemail PIN

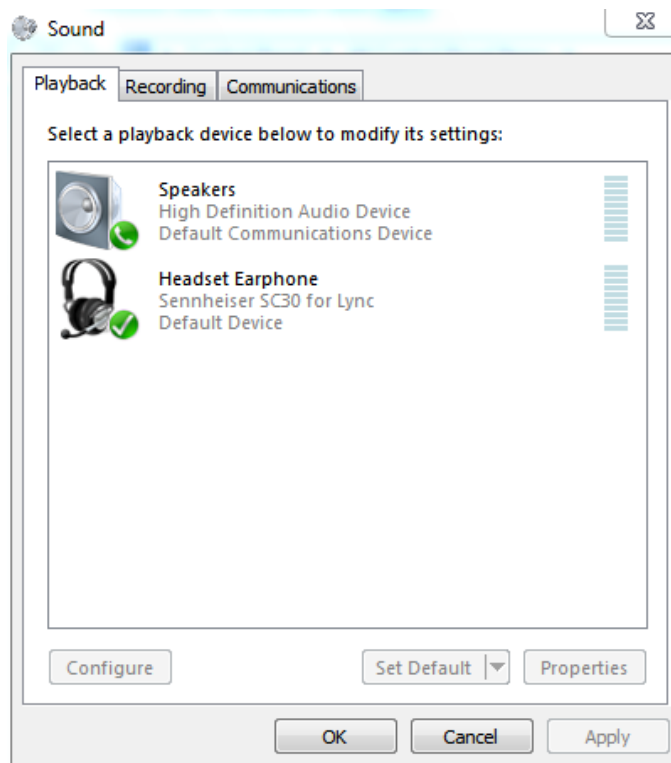
Please contact IT Helpdesk on 01484 414714 or 860 46888. This is the same number for any IT or Skype related issues.

Contacting people outside the Council

If you create a new contact in Outlook the contact will become searchable in Skype.

Voicemail sound

Occasionally, when playing back voicemails, they are played from your laptop speakers rather than your headset. To remedy this, simply click the Start button, click Control Panel and then open the Sound window. Set the headset as the "Default Device" by right clicking and choosing "set as Default Device" then set the Speakers as "Default Communications Device", again by right clicking and choosing "Set as Default Communications Device", so the windows looks like the one below:



What to Do in the Event of Loss or Theft of Mobile Working Equipment

Council equipment (laptops, PCs, printers) are insured against loss or theft, mobile phones are covered for unauthorised use – provided you take appropriate care of them and that you **report the loss or theft to the police within 24 hours**. It does not cover theft from an unattended vehicle and whilst you are travelling in the car our insurers advise you to keep the equipment in the boot out of sight.

Please bear in mind that although equipment is covered from a financial aspect, we need to take extra care of mobile equipment as they are likely to contain sensitive data or information.

If the worst happens and equipment is lost or stolen it's important that you follow the steps below:

- Step 1:** Report the incident to the police straight away (within 24 hours) and obtain a crime number.
- Step 2:** Contact EE directly to report it lost or stolen on **07973 100158** from a fixed line or 158 from a colleague's corporate mobile handset
- Step 3:** Contact IT to let us know that your mobile device has been lost or stolen so that we can:
- take necessary action to bar the device and protect our network
 - Contact EE if you are unable to
 - update the council's inventory
 - order a replacement device as quickly as possible
- Step 4:** Request an incident report form from Kirklees Council's insurance team on **01484 221000 and ask for Insurance** and pass it to your business support for processing.

Please also report the loss or theft to Councillor Support on: **01484 221000** or by email: councillor.support@kirklees.gov.uk

Details of the Mobile devices IMEI and telephone numbers will be provided to the user upon initial setup of the device in the form of a business card - These details will be required when reporting the lost/stolen device to the Police.

Please ensure that you keep any council equipment in a secure place overnight and when unattended.

Passwords

Kirklees passwords must contain:

1. At least one character that is uppercase (or in capital letters such as ABC)
2. At least one character that is lowercase (or in small letters such as abc)
3. At least one number (typed as a number such as 123)

If you wish, you can also use special characters such as:

` ~ ! @ # \$ % ^ & * () _ + - = { } | \ : " ; ' < > ? , . /

You will not be able to re-use a password until it has been changed 10 times.

Passwords now last 91 days, which means they will tend to expire on the same day of the week that you set them up. If you do not connect to a corporate PC or laptop regularly then we would recommend that you set up a diary reminder to change it on the first Wednesday of the month, for instance. This reminder could be sent via Councillor Support if you wish.

If you wish to change your password before the reminder prompt, just press:

<CTRL> <ALT> and <DELETE> together

You then get a menu with Change Password as one of the options; you may also use this technique to lock the device whilst switched on.

When you have changed your password on the network via PC/laptop you will be required to change it on DME as well, this will involve putting in the new password, you will be prompted that the password is unknown and ask if you wish to verify your login with the server, You should select Yes, you will then be prompted to enter the previous password for confirmation. You will have then realigned the passwords.

This is a link to a guide if you wish to read more about secure passwords:

<http://intranet.kirklees.gov.uk/Policies-and-procedures/Council-wide/Information-governance/Information-security/SecurePasswordGuide>

Please remember: Never let other people know or use your passwords. You are responsible for keeping them safe.

Feb 2018

Kirklees IT Equipment

Please note that equipment has been provided for your use only, it should not be shared with family members or friends. Any inappropriate use will be audited to you.

IT Support

Please note that IT provide a normal working day service from 7.15am until 5:30pm and can arrange visits between these times as long as planned with at least 48 hours' notice, outside of this we will try to accommodate requests

We currently provide a standby service for telephony support from 6am until 10:30pm week days and 7am while 7pm at weekends, plus 24 hour support for life and limb services.

The IT Service Desk can be contacted via the main switchboard on 01484 221000 or Councillors can ring direct on 01484 414728 (external) or 46883 (internal).

e-mails can be sent to eb.servicedesk@kirklees.gov.uk

If you need to collect or drop off a piece of hardware with us, Kirklees IT now has two office locations for your convenience: You can send it in the internal post or drop it off in person, between 10am-12pm and 2-4pm, at the following locations:

Red Doles Lane, Huddersfield , HD2 1YF – open Monday to Friday.

Empire House, Wakefield Old Road, Dewsbury, WF12 8DJ – open Tuesdays and Thursdays.

Electronic Communications Policy

Owner: HR Service
Author: Sharon Crane
Last updated: January 2012

Contents

1. Introduction	3
2. The use of the internet	3
3. The use of email and office communicator	4
4. The 'Sin Bin'	5
5. The use of the staff message boards	5
6. Misuse of electronic equipment	5
7. Monitoring and privacy	6
8. Breaches and sanctions	7
Appendix I: Classification of electronic communications misuse.....	8
Appendix II: Factors to consider	9

1. Introduction

All council electronic communications equipment is there to help provide a high quality service to our customers. The council allows employees and councillors to use the computer, email and internet for appropriate and moderate personal use. We trust employees and councillors to behave sensibly and to use equipment for personal use outside recorded working council time (for example, at lunchtime).

Where the council incurs a cost for personal use of electronic communications such as the telephone, mobile phone, fax and photocopying machine then personal use should be kept to a minimum and usually for emergencies only.

Use of electronic equipment often incurs costs for the council, for example text messages (even to other council mobiles) aren't free, this includes voice calls, SMS and MMS texts and any other types of messaging as well as premium rate and Orange 2-4-1 texts.

This policy covers the personal and work use of social media in the workplace. For additional advice about using social media as part of your work for Kirklees Council, please see our [Social Media Guidelines](#).

Failure to follow any aspect of this policy (either deliberately or accidentally) could lead to disciplinary action against you in accordance with the council's disciplinary policy which may result in dismissal.

2. The use of the internet

The internet is a valuable work resource, offering access to research data and other information sources. Users are expected to restrict internet access to work related sites within work hours. Reasonable personal use is permitted outside of recorded working council time (for example, at lunchtime). Any abuse of this privilege may result in disciplinary action.

Employees should not 'blog' using council's electronic equipment unless it is a legitimate part of their work. For example, management may use 'blogging' as a means of keeping their department up-to-date with the latest news from their service.

Following the removal of filtering blocks, employees now have access to many other resources, this means that social networking sites and webmail – such as Hotmail and Yahoo, facebook and Twitter are available. Kirklees recognises that employees have a right to a private life; however, we must ensure that confidentiality and our reputation are protected. We therefore require employees who use social networking websites to:

- Refrain from identifying themselves as working for Kirklees
- Ensure that you do not conduct yourself in a way that is detrimental to Kirklees
- Take care not to allow their interaction to damage working relationships between Kirklees, its partners and our residents.

Employees should not assume that their entries on any website will remain private.

Failure to follow any aspect of this policy (either deliberately or accidentally) could lead to disciplinary action against you in accordance with the council's disciplinary policy which may result in dismissal.

3. The use of email and office communicator

Email is provided as a work communication tool and any abuse of this privilege may result in disciplinary action. It must not be used to store or circulate personal email and any material that may be deemed by the council as offensive or discriminatory, or any material (including jokes, videos, pictures) that is actually or potentially defamatory of any person or organisation. For details of classification see appendix I.

Emails should be written in a professional tone and text, as they are a means of formal communication. Bear in mind that emails may be submitted as evidence in legal proceedings. The use of obscene language or swear words is prohibited. Please be aware that email discussions with third parties can constitute a legally binding contract. Use of the email system to copy and/or transmit any documents, software or other information protected by copyright law is prohibited without the appropriate copyright permission.

No email attachment should be opened unless you have absolute confidence in its origin as this is one of the most likely points of access of a virus into the council's computer systems. This includes material from a home email address. If you are in doubt, the email should be forwarded unopened to the Sin Bin.

Under no circumstances must an individual access the email of another individual within the council without express permission and a clear understanding of the reason for the proxy access.

Office communicator is our instant messaging, online chat, one click phone calls, video call system and also allows colleagues to know whether you are available, away from your desk or in a meeting and should be used in the same way you would use email.

4. The 'Sin Bin'

It is impossible to control what information is sent to a member of staff by email. However if offensive, obscene and/or discriminatory material is received it is then the responsibility of the receiver to do three things:

1. Forward the email to the 'Sin Bin' – sin.bin@kirklees.gov.uk

How? Highlight the email in your inbox and right click the mouse from the drop down menu, click on 'forward', type 'Sin Bin' into the forwarding box and click send. The email will then be considered by IT.

2. Delete the email from your computer
3. Inform your manager

Saving or not deleting emails and attachments that fall within this category is not only deemed offensive and is grounds for disciplinary action by the council but it also slows down computer communication by using up memory of computers and file servers.

5. The use of the staff message boards

The staff message boards are a facility on the council's intranet that allows employees to view and post messages relating to work and topics of general interest.

These boards must only be used during your own time (for example, at lunchtime), not during working hours.

- The staff notice board is intended for posting messages of general interest – not for chit-chat, gossip or jokes. Users can also enter into business-related discussions of a non-confidential nature.
- The 'unclassifieds' board is for staff to advertise private items for buying or selling. Please delete your message as soon as you have sold your item. No trade or commercial selling is permitted.

Bear in mind that your message has the potential to be read by many others and as such should be written in a manner that does not offend. It is all too easy for written comments to be interpreted in a manner that was not implied. Any abuse of this privilege may result in disciplinary action.

6. Misuse of electronic equipment

Misuse is a serious disciplinary offence. The following are examples of misuse and you MUST NOT:

- Store, view, download or distribute material that is obscene, offensive or pornographic, contains violent images, or incites criminal behaviour or racial hatred
- Gamble using council equipment

- Use council equipment, including the telephone, mobile phone, fax and photocopying machine, excessively for non work matters
- Undertake political lobbying (councillors are exempt from this provision)
- Promote or run a commercial business
- Download or distribute games, music or pictures from the internet for personal use. They can bring viruses with them, use up capacity on the servers and potentially breach copyright.
- Spend council time on personal matters (for example, arranging a holiday, shopping, looking at personal interest websites). This may be treated as fraud.
- Store personal information on your system or network that uses up capacity and slows down the system (for example, personal photos, screensavers or wallpaper)

- Send emails around the 'office' or team which:
 - are critical about a member of the team
 - contain specific or implied comments you would not say out loud in the team
 - contain inappropriate comments which could cause offence or harassment on
 - the grounds of gender, race, disability, age, religion or sexual orientation
 - have originated from a chain letter
 - Conduct private and intimate relationships via email

- Download or copy software
- Take and/or transmit pictures of a member of staff on your mobile phone, camcorder or camera without the person's permission
- Give away all-user email lists or lists of large number of email users for non-council business. If in doubt, ask your manager.
- Blog
- Use internet chat rooms

7. Monitoring and privacy

The council's email, internet and telephone facilities are business systems, owned by the organisation. The council therefore reserves the right to track all use of the the council's IT systems. Usage will be monitored to ensure that the systems are being employed primarily for business reasons, that there is no harassment or defamation taking place and that employees are not entering into illegal transactions.

Employees need to be aware that internet sites visited are traceable, and that deleted or trashed messages or attachments can be recovered.

Any material stored on the council's network or being circulated via the council's email system has no rights of individual privacy. In accordance with RIPA (Regulation of Investigatory Powers Act 2000) monitoring or surveillance without an employee's knowledge can be carried out on internal email systems, or information stored on a server. It is permitted to intercept communications in this way so the council can ensure its systems are being used properly in accordance with council policies and are working correctly.

The monitoring of email, telephone calls, mobile phones and internal and external post, unless clearly identified as private and confidential and not expected to be opened in an employee's absence, will be carried out on a regular basis. General monitoring of this

nature will be carried out in the normal course of the running of the council's business. As such, the monitoring would be regarded as falling outside RIPA as there is implied proxy access to all the council's communication systems for monitoring and interception of communications in order to deal with matters in an employee's absence for holiday, illness or other reason.

8. Breaches and sanctions

Failure to follow any aspect of this policy (either deliberately or accidentally) could lead to disciplinary action against you in accordance with the council's disciplinary policy which may result in dismissal.

Appendix I gives an explanation of the classifications used when investigating electronic communications misuse and is used as a guide. There may be material that does not readily fit into these categories.

Appendix II details the factors that are considered before deciding the appropriate sanction in cases of electronic communications misuse.

For information or any concerns you may have please contact:

- Your manager
- Your HR team
- IT Service Desk

Appendix I: Classification of electronic communications misuse

TERM	MEANING	RATING	SANCTION
Gross	<ul style="list-style-type: none"> • Time • Volume • Capacity • Offensive material of the following nature: <ul style="list-style-type: none"> o Sexually explicit or suggestive, usually in picture format o Racist o Homophobic o Ridiculing religion, disability, sexual orientation or politics o Ridiculing/demeaning individuals o Inciting cruelty or illegal activity 	Gross Misconduct	Dismissal
Serious	<ul style="list-style-type: none"> • Time • Volume • Capacity • Offensive material of the following nature: <ul style="list-style-type: none"> o Sexually orientated o Bad and offensive language o Politically aggravating o Ageism o Showing violence or nudity 	Serious Misconduct/ Misconduct	Final written warning/ written warning
Mild and non-offensive	<ul style="list-style-type: none"> • Time • Volume • Capacity • Material of the following nature: <ul style="list-style-type: none"> o Jokes/short stories with minor references to material of a sexist nature or in bad taste o Jokes/stories etc. of a non-offensive nature (that is, not gross, serious or mild) o Light hearted material o Cute animal pictures 	Misconduct	Written warning/ verbal warning/ informal process

Definitions

- **Capacity** – material that takes up a lot of capacity on the hard drive of the email account
- **Time** – personal use could be considered tantamount to fraud
- **Volume** – the numbers being received and/or sent on

Appendix II: Factors to consider

Factors to take into consideration before deciding the appropriate sanction in cases of email and internet abuse

If the allegations are proven, then consideration should be given to whether they are gross misconduct or other misconduct. Gross misconduct can be defined as misconduct for which dismissal would be appropriate without previous warnings. If the misconduct is not gross, then dismissal would not normally be appropriate without previous warnings.

Before reaching a decision on the appropriate sanction, the following factors should also be taken into account:

1. Seniority

Has the manager failed to set an example to the team? Has the manager challenged inappropriate behaviour amongst the team being managed?

2. Realisation of misconduct

Has the employee understood the implications of the breach of discipline?

3. Behaviour change

Is the employee likely to repeat the misconduct, or is a desired change in behaviour likely?

4. Coercion

Did the employee feel pressure to join in these activities, either through their peers or, more worryingly, their manager?

5. Instigator

Is the employee at the heart of the email abuse, encouraging and/or promoting the distribution of material?

6. Recipients

7. Policies breached

8. Environment

Have the images been viewed in an area where clients, service users or members of the public might be able to see it?

9. External contact

Has material been exchanged with those outside the organisation which would increase the risk of reputation of the council being damaged?



Information Security Policy

**Helping you safeguard council information,
equipment and reputation**

December 2011

The council's Management Board approved this policy on 12 December 2011.

Contents

Introduction

1. Organisational Security
2. Personal Security
3. Security of Information
4. Physical Security
5. Computer Security
6. More Information
7. Legal Context

Introduction

This Security Policy document summarises what is expected of all Kirklees Council employees in the course of their duties and while on council premises.

Its aim is to protect the council's customers, employees, assets (including information assets), finances and reputation by reducing the risk of:

- Harm to individuals
- Accidental loss or damage to assets
- Unintended change to, or disclosure of, personal and confidential information
- Deliberate and harmful acts carried out through lack of awareness of their consequences

It applies to:

- All services of the council
- All employees of the council, both permanent and temporary
- Councillors
- Any other person, or organisation, working for the council or on council premises

This policy document provides the information necessary to enable staff and others to meet their general responsibility to safeguard the council's information and other assets.

Personal Data and Sensitive Data

Any reference to **personal data** in this document means private information, whether in electronic or written form, about identifiable clients, employees, members of the public or any other persons. **Sensitive** personal data includes sensitive information about a living, identifiable individual for example, information which relates to their racial or ethnic origin, political beliefs or to their physical or mental health.

Detailed Guidance

Detailed guidance on all aspects of Information Security in this policy can be found on the intranet under Information security.

Government Connect

Kirklees Council has been accredited as Government Connect Compliant. This means that our infrastructure, technology and working practices have been assessed as secure, and we are able to use facilities provided by Government Connect for secure information exchange between the council and central government departments. This policy forms part of our compliance with Government Connect.

For further information and advice on information security and on this policy, contact the [Information Access and Security Officer](#)

1. Organisational Security

	Responsibility
1.1. The Management Board has a central custodian role on information security matters.	Directors and Assistant Directors
1.2. Senior management teams are responsible for implementing policy and advice.	Assistant Directors and Senior Managers
1.3. The Communications Board will direct, review, support and approve Information Security campaigns, advice and overall responsibilities. Its responsibilities are: <ul style="list-style-type: none"> • to recognise opportunities and risks • to flag up issues of concern • to coordinate effort • to review advice 	Directors and Assistant Directors
1.4. All managers and supervisors must ensure that those who report to them are aware of their general responsibilities in respect of security and the value of information, and of any issues or risks specific to their areas of responsibility.	All managers and supervisors
1.5. Information security should be a regular item on team meeting agendas to ensure that issues of concern are highlighted and addressed.	All managers and supervisors

2. Personal Security

	Responsibility
2.1. General responsibility for information security will be included in contracts of employment.	Human Resources
2.2. Checks on the career history (including criminal records) of job applicants will be made, appropriate to the responsibilities of the job.	Human Resources
2.3. Contractual arrangements with staff agencies will require similar, appropriate checks on agency staff.	Services
2.4. External contractors, consultants, trainers and others employed on council premises or given access to council systems must be subjected to checks and agreements appropriate to the services to be provided.	Employing managers
2.5. Work placements, students, volunteers, partners and any other persons not subject to the contract of employment, and having access to council premises and/or systems, will be required to sign confidentiality and security agreements.	Line managers
2.6. A record will be made of equipment, fobs, etc, issued to new employees and any of the above.	Line managers
2.7. Induction training will include security and data protection.	Line managers
2.8. Staff will wear ID badges at all times (unless otherwise agreed in certain circumstances).	All staff
2.9. On change of employment, access to computer systems and council property issued should be reviewed and returned or cancelled where appropriate. On termination of employment, all council property must be returned or accounted for, and computer system access cancelled.	Line managers

3. Security of Information

	Responsibility
3.1. It must not be assumed that information is a common resource to be freely exchanged	All
<p>3.2. Information is an important council asset. Much of the information held is available to individual members of the public under the terms of the Freedom of Information Act, subject to specific limitations and exemptions, in particular:</p> <ul style="list-style-type: none"> • personal data, which can only be disclosed to the person it relates to, unless there is consent or a legal requirement • information held in confidence • credit cards details, which must not be disclosed nor stored on paper, on computer systems or audio tape <p>All information, whether disclosable or not, must be protected from accidental or malicious loss and damage.</p> <p>Personal and confidential information must be protected from unintended access and disclosure and may only be disclosed to persons who can show they have a right to it.</p>	All employees, councillors and contractors
<p>3.3. Every personal data set routinely shared with an external agency must be the subject of a sharing agreement based on the corporate model adapted to the particular circumstances and the nature of the information to be shared.</p> <p>Each agreement will define the method of transmission and the security measures that will be employed to ensure the safe delivery of the information. IT can advise on the various methods of secure data transmission available. Responsible managers will rigorously enforce agreed security measures.</p>	Managers
3.4. A central register of all data-sharing agreements and data transfers will be established and maintained by the Information Access and Security Officer , and all existing and new agreements and arrangements will be notified to it.	Managers Information Access and Security Officer
3.5. Where there are formal data-sharing agreements with other organisations, managers must ensure that all staff are aware of the existence of any such agreements, and of their terms and scope.	Managers

<p>3.6. Personal data should not be accessed or viewed without legitimate reason.</p> <p>Under no circumstances will personal data held by the council be accessed, viewed or used for any private purpose.</p>	<p>All employees, councillors and contractors</p>
<p>3.7. Personal data should be stored on shared network drives (e.g. H: or G:) and not on a PC's C: drive.</p> <p>If the computer is 'stand alone' (not linked to a network), any essential data must be regularly copied onto alternative secure storage. Encrypted data sticks are available from the IT helpdesk.</p>	<p>All employees, councillors and contractors</p>
<p>3.8. No personal data should be held on laptop computers or portable storage devices (e.g. data sticks, mobile phones) for longer than necessary to carry out intended tasks, i.e. it should be deleted after use or transferred to network storage.</p> <p>Staff should ensure they are registered to use laptop encryption if they carry personal or confidential data routinely. No encryption or password facility should be used other than as specified by IT.</p>	<p>All employees, councillors and contractors</p>
<p>3.9. Personal data transferred to a shared portable device must be removed before the device is made available to another person.</p>	<p>All employees, councillors and contractors</p>
<p>3.10. Personal and confidential information in paper files or on removable media must be stored away at all times when not in use.</p>	<p>All employees, councillors and contractors</p>
<p>3.11. Electronic transmission of personal or confidential data should be via one of the two secure email systems available within the council.</p> <ul style="list-style-type: none"> • GCSx email – which should be used for sharing restricted and sensitive data with individuals from other public organisations (including other councils, central government bodies, NHS, police) who also have a secure GCSx email account. There's instructions on setting up a GCSX email account on the intranet or from the IT Service Desk. • Anycomms - which should be used for sharing sensitive information with any other organisation. <i>If you wish to use this method and either you, or the organisation you are</i> 	<p>All employees, councillors and contractors</p>

<p><i>transferring the information to, do not already have an Anycomms account then please contact the IT Service Desk.</i></p> <p>Ad hoc transfers of personal or confidential data to external agencies not otherwise covered by data sharing agreements should be avoided: where these are necessary then advice must be sought on the legal and technical mitigations that should be employed to protect the data, intellectual property, and to ensure the council's data protection obligations are properly met.</p> <p>In particular, personal and confidential data:</p> <ul style="list-style-type: none"> • must not be sent for purposes of "testing" whilst individuals can be identified • must not be sent or published using instant messaging, social networks, file sharing sites, external email or fax • must not be published or stored on any internet sites, or placed in any external hosted system under "general terms"; a formal council contract must be put in place or the terms formally reviewed by Legal Services • should only then be published where managerial guidance is available. This should clearly state the purposes and scope of any such publication, with due reference to the agreed terms, the council's obligations to follow the law, professional guidance and duties to protect staff and the public from misuse of information. <p>The sender is always responsible for verifying the intended recipients are who they say they are and are entitled to the information.</p>	
<p>3.12. Staff responsible for council PCs and laptops not permanently connected to the network are also responsible for regular back-up of data and for arranging for software patches to be applied and anti-virus and anti-spyware software to be regularly updated.</p>	<p>Managers, all employees, councillors and contractors</p>
<p>3.13. Documents containing personal or confidential information must be disposed of by shredding. This can be by services, through the confidential waste collection service offered by Document Solutions, or by an agency which can guarantee secure destruction. Paper containing personal data must not be recycled or used as scrap.</p>	<p>Managers, all employees, councillors and contractors</p>

<p>3.14. Documents, media, redundant PCs and similar equipment for disposal should be stored in a secure area until removed for disposal.</p>	<p>Managers</p>
<p>3.15. PCs, laptops and other devices must be disposed of through IT, which will ensure all personal data has been securely removed using specialist software.</p> <p>If PCs are to be re-allocated then IT will rebuild the machine in order to ensure secure deletion of any existing local data.</p>	<p>Managers</p>
<p>3.16. Data on disposable electronic media such as CDs and floppy discs, and any unwanted media containing personal data must be physically destroyed when no longer required, with due regard for personal safety, preferably using an appropriately designed shredder.</p>	<p>Managers, all employees, councillors and contractors</p>
<p>3.17. Any loss or damage to information, or equipment that may give access to information (e.g. ID cards, tokens, laptops, mobile phones , usb sticks) must be reported as soon as practicable to the IT Service Desk and to the Information Access and Security Officer</p>	<p>Managers, all employees, councillors and contractors</p>
<p>3.18. Any paper records taken out of the office must be treated with care, and extra care must be taken when destroying or disposing of anything outside a council location (e.g. at home or at a partner site).</p>	

4. Physical Security

	Responsibility
4.1. All council premises other than recognised public areas are 'controlled areas' for the purposes of implementing security policy.	Managers
4.2. Managers should be satisfied that access to the areas for which they are responsible is adequately controlled by their own or shared physical barriers or reception points.	Managers
4.3. Windows and doors allowing entry from uncontrolled areas must be closed and locked against external access when the location is unoccupied.	Managers, all employees, councillors and contractors
4.4. Visitors must be identified and supervised while inside controlled areas.	Managers, all employees, councillors and contractors
4.5. Staff should not allow unknown and unidentified persons access to any controlled area, e.g. by holding doors open. Anyone who feels unable to challenge a stranger should notify their manager or security without delay.	All employees, councillors and contractors
4.6. Computer screens should be positioned so they are not visible from outside the immediate work area	Managers, all employees, councillors and contractors
4.7. All staff must be alert to personal and confidential information in any form being visible beyond the immediate work area.	All employees, councillors and contractors
4.8. CCTV systems, where installed, must be the responsibility of a nominated person who will restrict access to recordings and ensure compliance with good practice	Managers responsible for CCTV installations
4.9. All staff must be aware of the possibility of bomb threats and premises managers must be aware of the procedure to follow. Public areas should be kept tidy so that objects out of place can be identified.	All employees, councillors and contractors

5. Computer Security

	Responsibility
5.1. Every user of a system should have their own user name and a set of rights appropriate to their work.	IT, system owners
5.2. Access to all computer applications must be controlled and protected by secure passwords.	IT, system owners
5.3. No external party, supplier, bureau, service provider or other agency may be given access to systems, data, hardware or networks unless an appropriate access agreement has been signed by them to ensure they understand their responsibilities.	IT, system owners
5.4. Passwords used to protect computer systems: <ul style="list-style-type: none"> • must be a minimum of 8 characters and include uppercase, lowercase and numeric characters • must not consist of purely dictionary words, personal names or words that have associations with individual users • must be changed regularly, or as required by particular systems • must not be shared with any other person • must not be written down in a manner discoverable by any other person 	All employees, councillors and contractors are responsible for ensuring that their own passwords meet these standards.
5.5. Computers should be logged out or the screens locked when left unattended. A 4 digit PIN should be set on all mobile phones and PDAs and the device should lock automatically after a short period of inactivity.	All employees, councillors and contractors. IT
5.6. All staff using mobile equipment, i.e. laptops and smartphones must be aware of the additional and significant risks of: <ul style="list-style-type: none"> • theft (including theft from council premises) • loss of equipment • information 'leakage' through being overlooked or overheard or interception • the opportunity for hacking presented by Bluetooth or Wi-Fi 	All employees, councillors and contractors

<p>All staff taking information and equipment out of council premises should:</p> <ul style="list-style-type: none"> • be aware of who is around when they use them • place council property away out of sight when not in use • not use Bluetooth on mobile phones and laptops • if possible use a direct cable or encrypted power line adaptor to connect to a network provider • use VPN to connect to the council network before surfing the internet • turn off Wi-Fi on return to the office and before connecting directly to the council's network. 	
<p>5.7. Working at home must be carried out with similar consideration for security as office-based working.</p> <p>Staff transferring personal data from council sources to their own computer, data stick or mobile phone etc are personally liable for the legal consequences.</p> <p>Encryption should be enabled for staff working in a mobile setting on council equipment to protect personal and confidential information wherever possible</p>	<p>All employees, councillors and contractors</p>
<p>5.8. Staff who choose to use their own home computers for ad hoc work purposes must ensure that:</p> <ul style="list-style-type: none"> • they have gained the agreement of their manager • they are not in breach of any formal data handling procedures which forbid use of personal equipment • the operating system and application software are patched regularly and that anti-virus, anti-spyware, and personal firewalls are installed and up to date • family members are not able to view data • data is transferred and deleted securely at the end of a working session 	<p>All employees, councillors and contractors are responsible for ensuring these standards are met on their own computers.</p>
<p>5.9. Emails that are obviously spam should not be opened, but sent to the Sin Bin.</p>	<p>All employees, councillors and contractors</p>
<p>5.10. Unexpected and unsolicited attachments to emails should not be opened and similar links to websites should not be followed.</p>	<p>All employees, councillors and contractors</p>

<p>5.11. No software should be installed or executed on a council owned computer without the agreement and assistance of IT.</p>	<p>All employees, councillors and contractors</p>
<p>5.12. No hardware should be installed or attached to the council network without the agreement and assistance of IT.</p> <p>This includes Bluetooth and Wi-Fi adapters, personal laptops, Ipods, personal cameras etc</p>	<p>All employees, councillors and contractors</p>
<p>5.13. Live personal data must not be used in the development of new computer applications, and may only be used in testing to verify consistency of output between an old system and its replacement or to assist in the resolution of an ongoing issue when all other options have been exhausted.</p>	<p>IT, system owners</p>
<p>5.14. Anyone becoming aware of an incident or event that could compromise the security of their computer should report it to their manager.</p> <p>Incidents must be also reported to the IT Service Desk and to the Information Access and Security Officer</p> <p>Such incidents include, but are not limited, to:</p> <ul style="list-style-type: none"> • the presence of intruders • exterior doors and windows left open inappropriately • unauthorised access or attempted access to computer systems • unauthorised access to personal data in any medium • accidental loss or disclosure of personal data • presence of a computer virus or spyware • equipment confiscated or inspected. <p>You can raise concerns in confidence under the Whistleblowing policy – found on the intranet.</p>	<p>All employees, councillors and contractors</p>

6. More Information

Data protection	Data Protection policy statement – found on the intranet
Information management	Search for ‘Information and knowledge management’ on the intranet
Forms (including access request, employee termination etc)	All forms are available on the intranet
Information security	Search for ‘Information security’ on the intranet
Personal Use (Use of Electronic Communications in the Workplace Policy)	Search for ‘Use of electronic communications policy’ on the intranet
Whistleblowing	Search for ‘whistleblowing’ on the intranet
e-learning courses on information security and data protection	Search on the Learning Management System (LMS)
Social media guidelines including a policy and code of conduct	www.socialmedia.kirklees.gov.uk

7. Legal Context

Data Protection Act 1998

Defines personal data and regulates all aspects of its use and processing.

Computer Misuse Act 1990

Prohibits unauthorised access to computer material, unauthorised access with intent commit or facilitate commission of further offences, and unauthorised modification of computer material.

Copyright, Designs and Patents Act 1988

Covers the copying of proprietary software.

Regulation of Investigatory Powers Act 2000

Part III: Investigation of electronic data.

Removable Media Policy for Kirklees Council

While recognising the use of removable media across the council is essential to our business needs, the introduction and use of unauthorised removable media can present a significant risk to Council Data. Kirklees Council has a duty of care to protect sensitive data and prevent the unauthorised disclosure of council information to unsolicited third parties and ensure the integrity of the data we maintain as stipulated in The Data Protection Act 1998. The use of unauthorised Removable Media also increases the risk to the IT Infrastructure through the introduction of malware, spyware or Trojans onto the network.

This policy is designed to provide information and advice to assist with the administration and use of removable media and provides guidelines for the controlled use of permitted devices.

Definition of Removable Media:

- USB Memory Sticks, also known as pen drives or flash drives
- Optical Disks such as CD and DVD Drives
- External Hard Drives
- Mobile Devices such as Smartphones, iPads, iPods, iPhones, Android devices and MP3 Players
- Digital Cameras
- Media Card Readers

Policy:

The use of removable media is not prohibited, but will be controlled and managed by the IT Services department for Kirklees Council. Any removable media that has not been authorised by IT Services will be available in a read-only capacity.

Writable USB Memory Sticks can be supplied, on request, by IT Services to ensure the security of council data through the use of 256 AES Encrypted devices which will be authorised and permitted for use. All other forms of unencrypted Memory Sticks, or pen drives will only be allowed in a 'read-only' capacity for use on Council workstations.

All optical disks, both fixed and removable, will be set to a 'read-only' state to reduce the risk of unprotected data being transferred to a CD or DVD disk and being removed from the council. Exceptions to this rule will be documented and regularly reviewed by IT Services.

Any sensitive council data stored on removable media is the responsibility of the officer who utilises the device and care must be taken to ensure the integrity and safekeeping of the data contained on the device. The data must remain encrypted and cannot be transferred using other methods to a non-secure location. In order to minimise physical risk, loss, or theft, all storage media must be stored in an appropriately secure and safe environment.

All officers who use encrypted Memory Sticks need to be aware that should they lose the password, then all data will be erased from the disk and the disk reformatted, therefore the encrypted removable media must not be used to store data that is not centrally secured and backed up elsewhere.

When using an encrypted memory stick or pen drive that has been supplied by IT Services, it must be protected by an 8 character complex password that adheres to section 5.4 of the [Information Security Policy](#).

Authorised encrypted removable media must only be used to conduct council business and cannot be used by any employee for personal use, or for the distribution of copyrighted materials.

All authorised and distributed encrypted Memory Sticks should be returned to IT Services when a member of staff leaves the council where IT Services will securely reformat the disk and re-distribute the device if necessary.

All workstations used by employees with authorised removable media devices must also contain regularly maintained and updated Anti-Virus software to prevent the transmission of malware between devices.

The use of removable media by external contractors, suppliers or temporary workers should be risk assessed before being authorised. The use of removable media devices by the general public will only be permitted on designated 'Public Access' workstations where additional security has been implemented to prevent any association with the council's internal IT systems.

Application of the Policy:

It is the policy of Kirklees Council to restrict the use of any unauthorised removable media and to ensure that secure methods of data transfer are adopted through the use of encrypted devices where possible.

All requests for additional access to removable media devices must be made through the IT Service Desk (860 46888 or it.servicedesk@kirklees.gov.uk) where advice will be provided. The use of any device that has not previously been authorised will require the completion of Removable Media Exemption Request Form and line manager authorisation to allow IT Services to assess the needs of the business and consider the impact.

Non-compliance of this policy could have a significant effect on the operation of the Council and may incur financial loss, reputational damage and an inability to provide essential services to our customers; therefore only in exceptional cases should a request be made.

Responsibilities:

It is the duty of all employees to inform the Information Security officer of any breaches, or suspected breaches to the security of the data held on an encrypted media who will, with the assistance of IT Services, investigate the incident.

It is the responsibility of IT Services for Kirklees Council to regularly review the Removable Media Policy and where necessary amend and update the information.

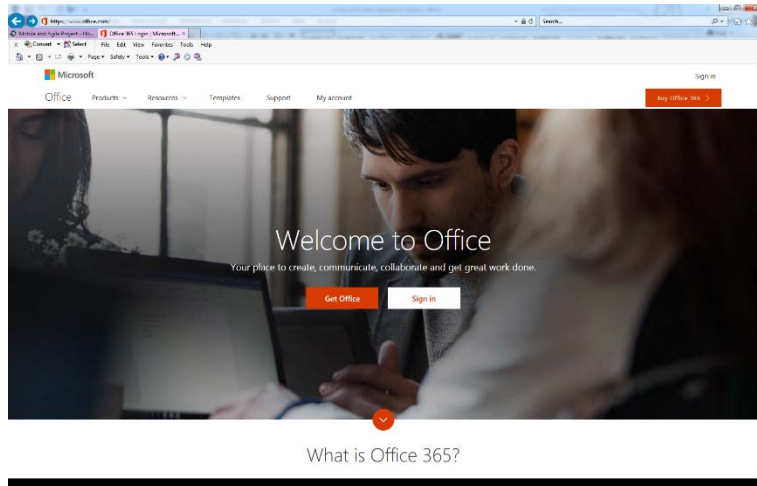
Members of staff are required to be aware of the Kirklees [Information Security Policy](#) and the Removable Media Policy enforces section 5.12. If additional access, granted via the above process, is no longer required, it is the requester's responsibility to inform IT Services so access can be removed.

Office 365 - How to update your 2 step verification mobile phone number

Use the following instructions if you want to update the mobile phone number you use to receive your 2 step verification code.

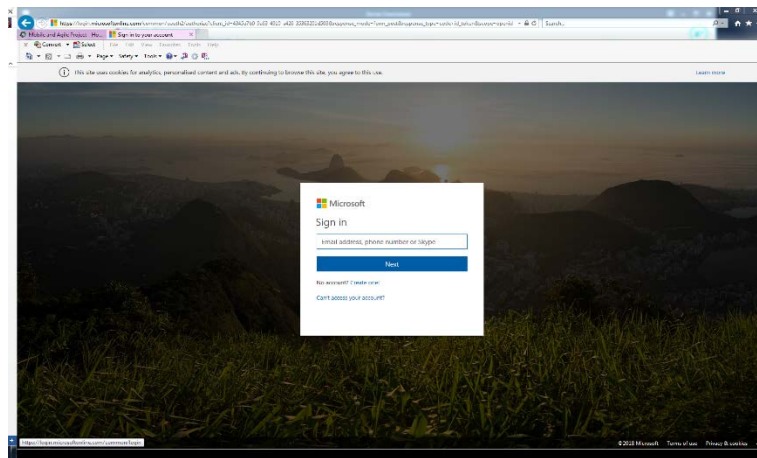
Go to [Office.com](https://office.com)

1



Click on Sign in

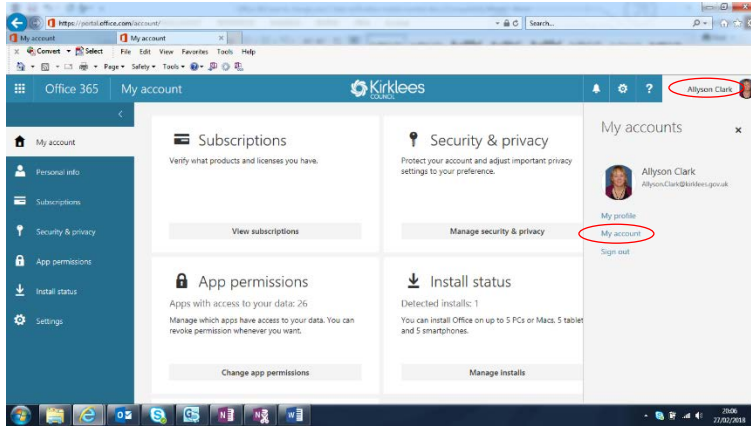
2



Enter your email address
e.g. firstname.lastname@kirklees.gov.uk or
@knh.org.uk if you work for KNH.

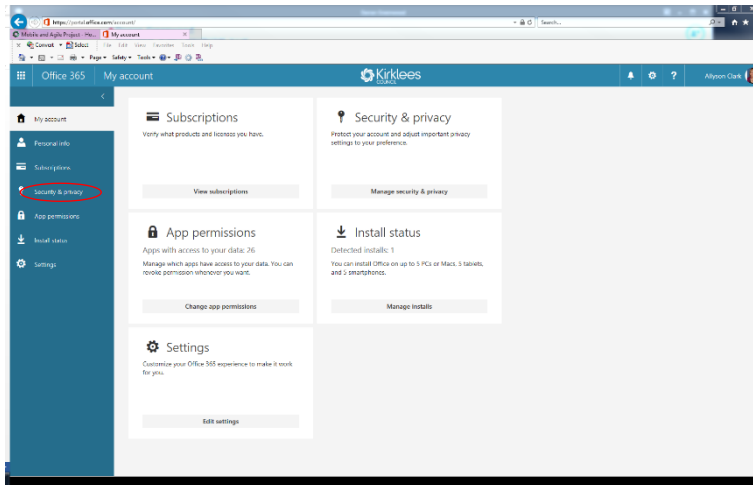
If you're not connected to the Council network you'll be asked to enter your password, use your usual password.

3



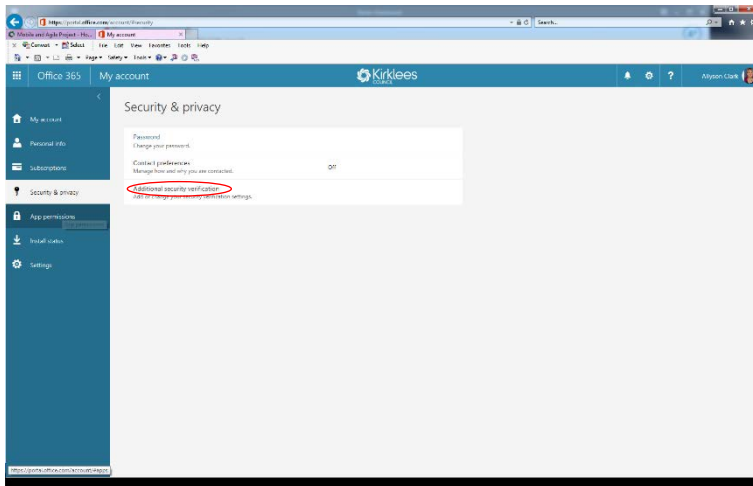
Click on your name and in the drop down menu click on My account

4



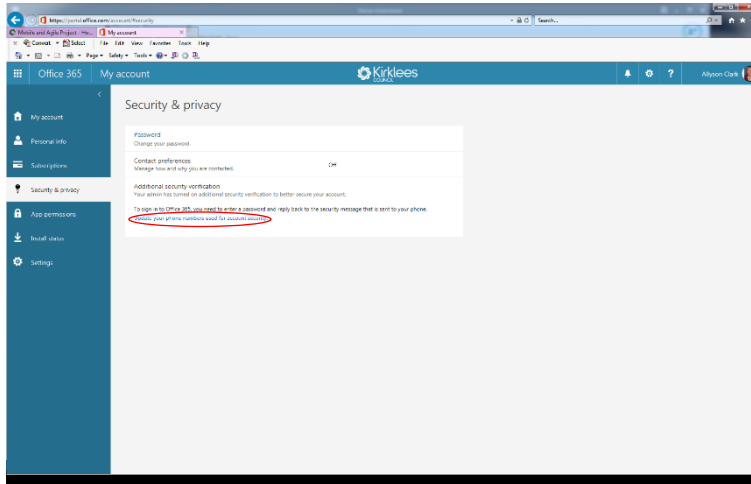
Click on Security & privacy

5



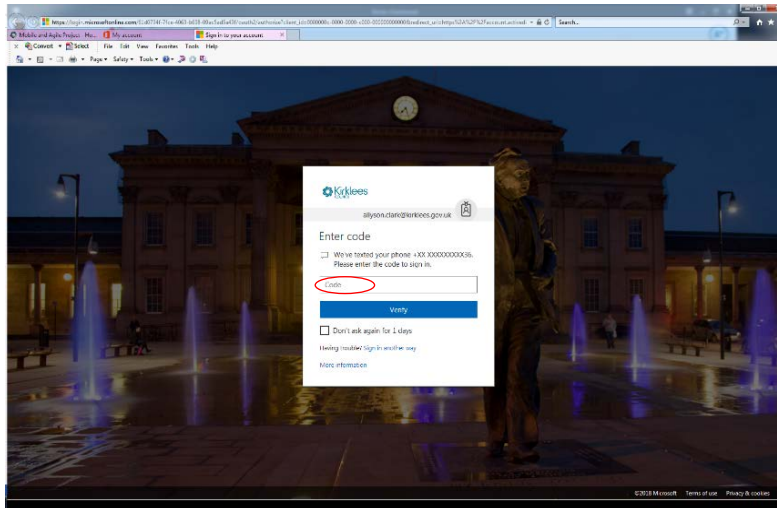
Click on Additional security verification

6



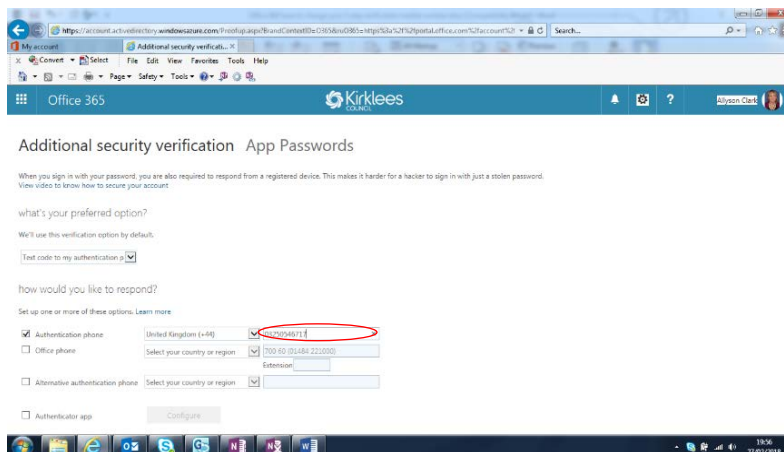
Click on Update your phone numbers used for account security
A code will be sent to your current mobile phone number

7



Enter the code sent to your phone and click on verify

8



Update your telephone number and click on Restore

9

Click on Sign out

