GUIDELINES FOR MOBILE DEVICES

RULES OF USE

Appropriate use

Any work-related calls can be made from your mobile phone. Calls to another Council employee will incur no charge so it is a very effective means of communicating with your colleagues.

Moderate and Reasonable personal calls can be made during working hours. Refer to Guide to Managing Discretionary Expenditure

Use your mobile phone responsibly and safely. When you first receive it set up a personal identification number (PIN) to protect against any unauthorised use.

Your mobile phone is provided as a business tool - much like your computer. If you leave your mobile phone at home, the IT Service Desk will provide you with a temporary loan phone for use during working hours subject to availability. You should also make sure that your phone is charged at all times.

Notes:

- please be considerate of your colleagues when selecting the volume and ring tone for your mobile. Where possible, select vibrate or meeting mode to minimise disruption
- you will be able to access mCommerce services (eg TXT-a-Park) from your mobile. You should discuss the use of these services with your manager prior to accessing them and any purchases for personal use must be reimbursed. Refer to Guide to Managing Discretionary Expenditure and Reimbursement and Billing.

Inappropriate Use

The following examples could result in a breech of the Code of Conduct. Please note this list is not complete, there may be other actions that are not listed below that are in breach of the Council's Code of Conduct.

- Sending personal PXTs to your work Council email account as this may affect our IT network.
- Using your mobile connection in a way that could bring the Council into disrepute. Eg: Posting unofficial information to Facebook using your mobile
- Lending your mobile connection to friends and/or family members.
- Continually spending above your monthly threshold without approval from your manager.
- Providing misleading information about your phone or datacard being damaged, lost or stolen.
- Frequently leaving your mobile phone at home so it is not available for use at work.
- Using your mobile connection to conduct business activity not related to the Council (eg operating your own company).
- Using your phone for 0900 and international calls. Management approval will be given to those who need access to these for work purposes.
- Excessive personal use not in line with Discretionary Expenditure Guidelines and not supported by personal reimbursements

Security

Business Unit Managers are responsible for ensuring their staff are aware of the security implications of using Mobile Devices and that they are fully trained in their proper use.

Devices must not be connected to Council Systems unless appropriate security controls have been installed and approval has been obtained from the Group Manager IT Operations.

Devices must be protected by a PIN or password that meets the Council standards. Refer to Password Guidelines.

All Council information stored on Devices must be encrypted. This is to protect against data being view by unauthorised parties due to loss of theft of devices

All Laptops must be protected by boot passwords. This is to protect against unauthorised parties gaining access to your device.

Any data must not be copied to devices directly via a USB cable, unless that device has full device encryption. This will stop the possibility of unsecured data on devices being accessed by an unauthorised user.

Bluetooth Devices must be configured as non-discoverable and "paired" between specific Devices such as a cell-phone and a laptop. Bluetooth Devices must not be configured to advertise themselves to any other Device.

Infrared or bluetooth functionality must be switched off when not in use. Information transferred via these methods can be intercepted and read by another device.

Any mobile device connecting to Council must not allow the Operating System to be compromised allowing privileged control. Proactive detection of security breeches is in place and any devices found to have this will be denied access.

Anti Virus and Copyright

Council Devices must not be used to download Software from any non-Council Systems – this includes the Internet. Software can contain viruses and other malware that can damage Council Systems. If you need to download software, contact the IT Helpdesk.

Software must not be stored nor run on any Council Device or Council Systems without Business Unit Manager approval. Note that Software includes music or video files. Software use may impact on the Council data plan; Council data storage is limited and there is a cost to Council if it needs to be increased; Council also needs to observe music and video copyright law.

Business Continuity

If critical information is stored on a Device it must also be backed up. Major changes to critical data must be backed up immediately. The backups must be stored separately from the device in a safe location and not in the same bag in which the Device is carried. As soon as practicable, critical information must be transferred to the Council document management system.

Council Systems

The allocation of Council Devices must be approved by a Business Unit Manager. Note that as at July 2012 Council will no longer be allocating Symbian-based phones as data cannot be encrypted on these phones.

Devices must require the user to successfully identify and authenticate themselves before access is granted to the Device. Council Systems may also require additional authentication depending on the sensitivity of the information being accessed. Devices are sometimes used in public spaces such as at conferences and in cafes where there is potential for the device to be misplaced and for access to occur by an unauthorised person. Authenticating separately to Council Systems helps reduce or eliminate the risk of unauthorised access to Council Systems and data.

Devices must only be connected to Council Systems by methods approved by the Group Manager IT Operations.

Devices must not be attached to, connected to, nor synchronised with Council Systems without Group Manager IT Operations approval.

Devices must connect to the Council network from outside the Council firewall. This keeps Council Systems secure. It also allows a seamless experience when roaming to another location such as to a home wireless network or a cafe WiFi. This keeps information secure, as no information is stored on the local device.

Access to Council Systems and information in Council databases may be updated only where:

- strong authentication controls have been established
- Group Manager IT Operations approval is obtained
- the connection is via Council Remote Access.

Where available, Devices must use WiFi networks as the primary connection to Council rather than mobile networks as this saves on mobile data charges.

When connecting to the Internet using Council Systems the Internet Use Policy applies.

Work-related music and video must be stored on EDRMS or your business units G: drive.

A lost of stolen Device under Council control must be reported to the Council IT helpdesk as soon as possible.

Council Devices must not be changed or added to in any way such as upgrading or downgrading the processor, memory or functionality without Group Manager IT Operations approval. Only IT Help Desk staff may carry out such changes.

Personally Owned Devices (BYOD)

To use your personal phone for Council business, you must use a Council SIM card. This enables the Council standard numbering plan to be maintained and allow correct billing for calls. This also has the advantage of being able to call fellow staff for free (And vice versa). The Council does not support “bring your own number”.

You must not use the Council cellular network for personal data. For example, browsing the internet or applications as a cost is incurred by Council for this. Any personal use must be done through the WiFi network.

To use Council email on your phone, you will need to agree to your device being locked-down and under the control of Council. This will limit some functionality of your device. This ensures security and continuity of Council information can be maintained.

If your device is lost or stolen and under Council control it will be remotely wiped to ensure Council data cannot be viewed or copied by unauthorised users. This may result in the loss of personal data such as photos and TXT messages.

If Council believes your device poses a security threat to Council Systems or if any Council policy is not complied with Council can refuse to connect or disconnect your device from Council systems.

Your device must have anti-virus software installed and regularly updated. Auto-updates via networking must be enabled where this is supported by your device.

Recommended software:

- ANDROID – AVG. Free from Google Play store
- iPad and iPhone – http://www.intego.com/virusbarrier-ios.

Once access is no longer required or you leave Council employment, all Council data, software and configuration settings will be wiped from Your Device. Depending on the device type, this may mean a complete wipe back to factory settings which may result in the loss of personal data such as photos and TXT messages.

Symbian-based devices are not supported as data encryption is not available, this leaves Council data vulnerable to unauthorised access

Support is on a best endeavour basis. Requests for service will only be performed if and when IT Helpdesk workload permits.

HARDWARE

Mobile Phones

As an eligible employee you will be provided with a handset including a battery and a battery charger.

Other accessories are available for a charge to your Business Unit eg hands-free kits, extra mobile phone chargers. Refer to Mobile Phones intranet page.

Important: Any issued mobile connections and accessories remain the property of the Council.

SIM Cards

Your mobile phone will come with a SIM card. A SIM card is a microchip that carries all your information: your network ID, numbers in your address book and more. If you change mobile phones, you can transfer your SIM card to the new phone and it will automatically take on your phone number and address book. All important numbers should be stored on the SIM card.

Important: Any issued SIM card remains the property of the Council and cannot be kept if you leave Council employment.

Data Cards

A data card is a modem card that fits into laptops. This enables connectivity to the internet allowing staff to view emails and Council databases. Datacards can only be used with Council laptops for business use.

Ensure you secure your data card against theft and damage when unattended.

REIMBURSEMENT AND BILLING

Personal Use Reimbursement

A monthly threshold will be set to assist you in monitoring your mobile connection usage. This threshold will be decided between you and your cost centre manager. If your monthly bill exceeds your threshold, your cost centre manager will approach you to review business and personal usage.

Personal use above the threshold needs to be reimbursed.

Discuss with your cost centre manager the most appropriate option or combination of options to make your payments:

Payment option of...	may be suitable if you...	How are you charged?
casual reimbursement	make occasional calls, TXTs or PXTs.	Reimbursement for actual use
deduction of a set amount	call and TXT or PXT.	Automatic deduction from your pay

Refer to Guide to Managing Discretionary Expenditure

Note: You will need to discuss your threshold amount with your cost centre manager prior to going on leave as it will be expected this will be lower than your normal working threshold.

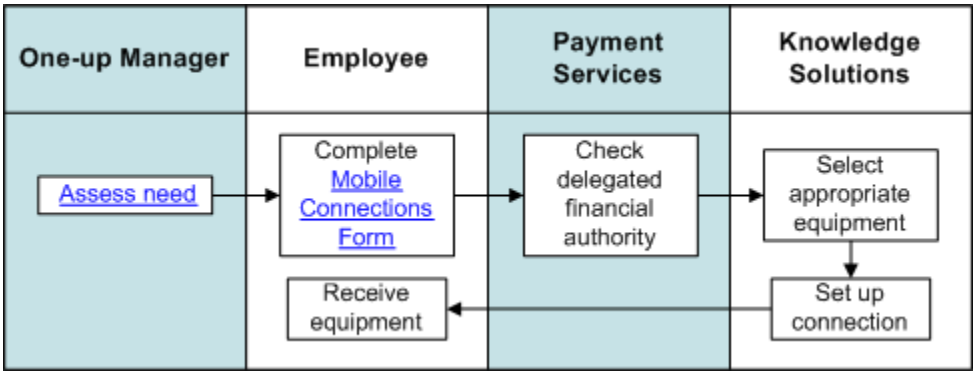
Billing

All connections will be set up under the Council staff account in your name and cost centre. Monthly bills will be sent to your cost centre manager for authorisation. You must complete the Mobile Connections Form if your cost centre and/or DDI number changes.

GETTING CONNECTED

Procedure

Use this procedure to arrange a new or replacement mobile connection:



For detailed specifications on standard mobile phones, data cards and other mobile equipment that IT supplies and supports, refer to Mobile phone webpage.

Assess Need

When deciding on the type of phone for an employee, one-up managers must consider whether the employee:

- needs to be immediately contactable
- is regularly away from their desk for extended periods
- generally works off-site
- has a mobile phone and/or mobile data connection specified in their remuneration package
- needs a temporary or permanent connection
- can be contacted in a more cost effective way.

Maintaining your Connection

Changing your details and leaving the Council

If you...	Then you must...
Are changing cost centres or business units	Notify the IT Service Desk by filling in the Mobile Connection Request Form (Online I PDF)
No longer require mobile connection for your role or have been upgraded to a new model	Fill in the Mobile Connections Form and return with your mobile connection and any accessories.
Are leaving the Council	Fill in the Mobile Connections Form and return with your mobile connection and any accessories on your last day of employment.

Refer to Exit Checklist.

Repairs, Maintenance and Access Problems

If your mobile phone is damaged or you have problems accessing the network, contact the following:

Description	Action
Damaged mobile phone	• Contact the IT Service Desk during the hours of 7.30am to 5.30pm Monday to Friday. • If the issue occurs outside these hours phone Vodafone on 0800 800 021 or 777 from any Vodafone connection.
Problems accessing the Vodafone network	• Contact the IT Service Desk during the hours of 7.30am to 5.30pm Monday to Friday. • If the issue occurs outside these hours phone Vodafone on 0800 800 021 or 777 from any Vodafone connection. • Complete the Vodafone Network Performance Form and send it to the IT Service Desk.

Notes:

- All repairs and maintenance costs not covered by the warranty will be paid for by the Business Unit.
- If your mobile phone is damaged beyond economical repair, you will be provided with a replacement phone.

Lost or Stolen Phones

You will need to call the IT Service Desk immediately to have the phone and the number blocked from the network. If the incident occurs outside the hours of 7.30am and 5.30pm Monday to Friday, call Vodafone on 0800 800 021 (or 777 from any Vodafone connection) as soon as possible so they can block the number and the phone.

Lost or stolen mobile phones must be reported to your manager and to the Police as soon as possible. It is important to get a police report from the Police outlining the incident for insurance purposes.

Your business unit may be charged for a replacement phone. The IT Service Desk will contact your cost centre manager prior to ordering a new phone.

If your mobile phone is subsequently found, please contact the IT Service Desk as soon as possible.

Refer to Insurance Policy.

Health and Safety

The Council promotes safe driving practices. Make sure your vehicle is stationary and parked safely before using your phone. If this is not possible, let your voicemail pick up the call and return the call when it is safe to do so. Refer to Using Council Vehicles Standard.

For more health and safety information on mobile phones refer to Vodafone's Mobile Phones and Health page.

Upgrades

Employees are not entitled to an upgrade unless their role changes and they require additional mobile functions. Refer to Getting Connected.

Registering to check Vodafone usage on-line

1. Visit HTTP://www.vodafone.co.nz/business/
2. Click on "Register for my account" (on the right side of page)
3. Complete the registration form with the requested information
    a. Tip: the Vodafone number should be in 021xxx xxxx format
    b. Next
4. "We've sent you a text" page
    a. Enter the validation code which was sent to your mobile device
    b. Continue & next
5. "Setting up access to your account or mobile device page
    a. Choose the last option "I am an employee with permission to view my mobile device"
6. "Registration completed" page
    a. Your on line ID has been created, your username is your email address
    b. Click on "view account summary" to view your details

Mobile Phone Tips and Hints

Good general mobile phone tips and hints and costs can be found here:
http://staffnet.net.ad.wcc.govt.nz/phones/

But costs in summary:

Mobile Phone Charges

Call Destination	Cost per minute or item (plus GST)
To Civic Square Campus	No Charge
To Council 021 mobile	No Charge
From Civic Square Campus desk to WCC mobile	No Charge
To Non-Council 021 mobile	15c per min
To Non-Council 027 and 022 mobile	25c per min
To Wellington local call or Non-Campus Council Office	6c per min
To New Zealand national call	6c per min
Text Messages (from Vodafone 021 to Vodafone 021)	17c each up to 8.84 then no cost up to 1000 messages per month to Vodafone network only.
Text Messages (to non-Vodafone)	17c each
PXT messages	44c each
Monthly Mobile Access charge	$22.00 per month

WCC Landline to Telecom mobile	25c per min

Voicemail Call Back Charges
Using the Call Back Feature via Voicemail incurs charges. The charges will apply when calling back Council talk Zone numbers and non-Council numbers. To prevent being charged, end the voicemail call and make a separate call to the number.

Manager's Visibility to Mobile Activities
The invoice provided to Council each month itemises all calls made from each Council phone.

Billing details and queries
Please contact Derek Waldock on ext 8655 for any billing enquiries regarding your phone service.

Calling Overseas
It is Council policy that overseas calls are barred without one-up management approval.