Birmingham City Council

Standard for the Use of Mobile Telephony

If you have any enquiries about this Standard, contact the Information and Strategy Team on 0121 675 1431 or 0121 675 1429.

Standard Owner:	Jackie Woollam Head of Strategy and Governance Birmingham City Council
Author:	Dave Thomas Strategy and Governance Birmingham City Council
Version:	3.0
Date:	31/01/2018
Classification:	OFFICIAL

CONTENTS

1. OVERVIEW AND PUBLICATION PARTICULARS

Document History

Version	Date	Purpose	Author
0.1	20/02/2013	Initial Draft	Caroline Hobbs
0.2	07/03/2013	Revised Draft	Gerry McMullan
0.3	15/05/2013	Final Draft	Gerry McMullan
0.4	11/04/2014	Revised Final Draft	Gerry McMullan
1.0	15/05/2014	Revised Final	Gerry McMullan
1.1	13/06/2017	Revised Draft	Dave Thomas
1.2	21/06/2017	Updated Draft	P Giann, M Blizzard, J Coley, V Lewin
1.3	04/07/2017	Revised Draft	Dave Thomas
2.0	12/07/2017	Final	Jackie Woollam
2.1	30/01/2018	Revised draft	Dave Thomas
3.0	31/01/2018	Final	Jackie Woollam

Document Distribution after Approval

Name	Organisation
All Staff	Birmingham City Council
All Staff	Capita ICT & Digital Solutions

Document Reviewers

Name	Organisation	Team
P Giann, J Coley, V Lewin	BCC	Information, Technology and Digital Services

Overview

Authority[1]	Birmingham City Council – CIO & Assistant Director Information, Technology & Digital Services
Owner[2]	Birmingham City Council – Head of Strategy & Governance
Scope[3]	This Standard applies to all Birmingham City Council mobile and fixed telephony and the users of the these systems/devices.
Review period[4]	This document will be reviewed at least annually or more often if justified by a change in circumstances.
Related Birmingham City Council documents	Telephony Best Practice Guide 2017 Information Security Incident Response Standard
Related Capita ICT & Digital Solutions documents	Telephony Liaison Officer Roles and Responsibilities Good Practice Guide for Mobile and Landline Telephony Blackberry Reallocation procedure Mobile Recycling process
Legislation or Regulatory Control references e.g. BS ISO/IEC 27001:2013	None identified

[1] AUTHORITY: The person or organisation who is responsible for enforcing this standard

[2] OWNER: The organisational position of the person who has rights to authorise changes to, or disposal of, this standard

[3] SCOPE: The organisations or persons to whom the standard applies

[4] REVIEW PERIOD: How frequently the standard should be reviewed

2. PURPOSE OF THE STANDARD

This Standard governs the use of all mobile and equipment supplied by Birmingham City Council or used for council business purposes.

In this Standard, “mobile devices” is taken to cover devices which can transmit and receive data traffic as well as voice traffic – such as smartphones and tablets.

3. STANDARD PARTICULARS

Purchases, Reallocation and Disposal

All new mobile, fixed and data connections must be procured via Capita ICT & Digital Solutions , who should always be contacted when new requirements are identified. Each directorate has a nominated Directorate Telephony Liaison Officer who is the key contact within their business area for the monitoring and control of the telephony estate.

If any equipment becomes surplus to requirements, it must be reallocated wherever possible. The Directorate Telephony Liaison Officer is responsible for managing the Directorate reallocation process.

If a device is not suitable for reallocation, it must be disposed of using the agreed procedures available on the SB Portal. Responsibility for arranging disposal lies with the Directorate Telephony Liaison Officer.

Capita ICT & Digital Solutions maintain a record of all mobile user and account information.

Lost or Stolen Equipment

The individual mobile user is reponsible for notifying O2 Customer Services of the lost device and its number imediatley. Capita ICT & Digital Solutions and the Directorate Telephony Liaison Officer must also be notified of any lost or stolen equipment at the first possible oportunity. All new equipment must be procured via Capita ICT & Digital Solutions (see above).

Special Requirements

Any special requirements should be discussed with Directorate Telephony Liaison Officer and Capita ICT & Digital Solutions early in the procurement process.

Choosing the appropriate device

Mobile devices chosen should be appropriate for the type of use that is needed for that employee. In particular, smartphones should not normally be purchased where there is no requirement to manage e-mail or to send and receive data. High value telephony devices will require a business case to be

submitted and agreed by Directorate Telephony Liaison Officer before an order will be processed.

Billing

Users and their service managers are responsible for checking the accuracy of bills relating to the devices supplied to them. Billing information is available on request.

Personal Use

As per the HR Code of Conduct, personal telephones can only be made when necessary and within reason. Personal use must be monitored and any costs of calls incurred repaid using the appropriate or corporate procedure for recovering payments.

Emergency Use

Mobile devices and can be used to make emergency calls if necessary. The 999 emergency services number can be used from mobile devices, but some also have other emergency settings. Users should familiarise themselves with the settings for the device they are using.

Driving

Mobile telephony must never be used when driving, and ideally should be stored in the boot of the car. This is covered by the corporate policy on driving, which is published on People Solutions.

Use of Mobile Devices Abroad

Mobile phones may be used abroad for business purposes only, subject to approval by an appropriate manager. Contact Directorate Telephony Liaison Officer for advice on what action needs to be taken before travelling.

Transferring calls to mobile devices from Landlines

Landline numbers may be transferred to mobile devices where no costs are incurred for the call to aid agile and mobile working.

Security

All mobile assets must be tagged. Tags must not be removed from devices. SIM cards must not be transferred to non-approved or personal handsets. This may result in loss of service due to security and may have cost implications. Problems with handsets other than technical ones must be referred to the appropriate Directorate Telephony Liaison Officer.

3G/4G

3G/4G services will be provided wherever it is cost-effective do to so. However, their service availability is not always guaranteed.

Public Wi-Fi Security

Many coffee shops, hotels, shopping centres, airports offer free access to public Wi-Fi, it's a convenient way to check your emails, catch up on social networking or surf the web when you're away from the office. However, cybercriminals will often spy on public Wi-Fi networks and intercept data that is transferred across the link. In this way, the criminal can access users' banking credentials, account passwords and other valuable information.

- **Be aware**
  Public Wi-Fi is inherently insecure — so be cautious.

- **Remember —** All devices could be at risk and susceptible to the wireless security threat.

- **Treat all Wi-Fi links with suspicion**
  Don't just assume that the Wi-Fi link is legitimate. It could be a bogus link that has been set up by a cybercriminal that's trying to capture valuable, personal information from unsuspecting users. Question everything — and don't connect to an unknown or unrecognised wireless access point.

- **Try to verify it's a legitimate wireless connection**
  Some bogus links that have been set up by malicious users — will have a connection name that's deliberately similar to the coffee shop, hotel or venue that's offering free Wi-Fi. If you can speak with an employee at the location that's providing the public Wi-Fi connection, ask for information about their legitimate Wi-Fi access point — such as the connection's name and IP address.

- DO NOT use Public Wi-Fi to transfer Personal / Sensitive data.
  If you need to access any websites that store or require the input of any sensitive information including social networking, and online banking sites DO NOT use Public Wi-Fi. Access must always be gained via your corporate laptop with the additional security of the Netmotion connection.

- **Avoid using specific types of website**
  It's a good idea to avoid logging into websites where there's a chance that cybercriminals could capture your identity, passwords or personal information, such as social networking sites, online banking services or any websites that store your credit card information.

4. ROLES AND RESPONSIBILITIES

Role	Responsibilities
Birmingham City Council Corporate Management Team and Directorate management teams	• To support the implementation of this Standard
Birmingham City Council IT&D Service	• To ensure this Standard meets the business need and is reviewed annually • To oversee the Telephony process and be the central point of contact for Capita ICT & Digital Solutions and Directorate Telephony Liaison Officers • To disseminate this Standard within Birmingham City Council
Capita ICT & Digital Solutions	• Provide a managed telephony service for Birmingham City Council • Procure all mobile telephony for Birmingham City Council • Advise on specific mobile telephony requirements • Maintain an asset register and user/account details for all mobile telephony users
Directorate Telephony Liaison Officer	• Monitor and control the procurement of mobile telephony (including non-standard) • Review quarterly and update Capita ICT & Digital Solutions. • Produce and disseminate quarterly bill reports depending on directorate requirements • Identify connections no longer required (from zero usage on billing) and raise cease requests • Manage the reallocation of existing mobile equipment. • Arrange disposal of surplus devices via Capita ICT & Digital Solutions • Monitor and control lost or stolen devices.

6. EXCEPTIONS

There are no exceptions to this Standard

7. ENFORCEMENT

Any individual member of staff who contravenes this Standard may be investigated under the Council's disciplinary procedure and, where appropriate, legal action may be taken.

Other individuals within the scope of this Standard may be investigated and, where appropriate, legal action may be taken against them, or withdrawal of privileges. Third parties or partner organisations who contravene this Standard may jeopardise their relationship with Birmingham City Council and may also face legal action.

There is a city wide best practice mobile telephony guide that sits alongside this document and is available on the Intranet.