# 10.15 Information Systems Access Policy

# Policy statement

Access rights should be granted based on least privilege necessary to perform the job role, to assist in preserving data security. Access controls are critical to the protection of information entrusted to CAPITA by the LBB. Through restricting access to information on a need to know basis, these measures will enable CAPITA to provide assurance to LBB that only authorised users have access to required information whether at a physical, electronic, application, network or operating system level. Volunteers can be granted access if it is required for the volunteer role they are filling. Access will only be granted if all other relevant checks have been satisfactory completed (DBS etc).

**Core elements for Children Centre Staff**

All children centre staff should adhere to the corporate Information Systems Access Policy which is available on the intranet and as a hard copy within each Children Centre. The core elements of the policy that Children Centre staff are likely to engage with are:

**User Network Accounts**

1. ***New Users/Changes: Barnet Council & The Barnet Group***

On joining LBB a user will be set up with network access on confirmation of employment by the HR department. The process is initiated by the HR department who will inform the IS service desk daily of any new user account required and provide the required detail.

Requests from HR will be treated as an authorised request to enable the account to be created which will be logged and recorded via a service request.

Some access to systems and data will be pre-approved as part of the New Starter process. These “Standard Changes” include provision of a user e-mail account, user Home drive, access to fixed telephony, and the default shared drives where agreed. The process will include the creation of a service desk account for the user. On setting up the account a one-time password will be used and the user will be forced to change this at first log on in accordance with the password policy.

This process applies for all users, including permanent staff, contractors, agency staff and interims.

Changes to employment resulting in movement between teams or delivery units will be notified to HR by the relevant line manager who will in turn notify the IS service desk. Service desk will generate service requests to control any resulting changes required.

All mover requests must be treated in the same way as a leaver or new user registration. Access to all systems must be removed and only those drives and systems appropriate to the new role added to the user profile.

In the case of long term sickness or maternity leave, network access will be suspended on notification by HR and reinstated on return to work.

1. ***Third Party Access***

Network accounts required by third parties for application support must be requested by system owners by a service request. Such accounts will only have the privileges required to support the application and will have no additional facilities such as e-mail, user home drives etc., unless authorised by exception.

1. ***Leavers***

On leaving LBB a user network access account must be closed. This will remove right to access all facilities and information on the Barnet network. For Barnet Council and The Barnet Group staff, the leaving notification is initiated by HR who will provide the IS service desk with the details of the leaver. This request will be logged and recorded via a service request, and the account will be disabled at the appropriate date. The AD account will be set to automatically expire at the end of the last day of employment.

This applies whether the user is a permanent employee or a contractor on a temporary or part time contract with LBB.

**E-Mail systems**

***a) Overview***

Standard e-mail accounts are provided as part of the new starter process. In addition to the standard e-mail system, LBB also has access to GCSx mail systems used for conducting secure communication with the police, NHS and government departments.

GCSx accounts can be provided through a service request. Users of GCSx mail will be required to accept an additional set of terms and conditions as part of the setup process.

To send secure communications to external partners who do not have access to GCSx mail, the Message Labs “Encrypt and Send” service must be used. Message Labs secure mail can be provided through a service request.

***b)*** ***Controls***

On leaving LBB a user network account will be closed, which includes access to E-mail. This applies whether the user is a permanent employee or a contractor on a temporary or part time contract with the London Borough of Barnet.

E-mail accounts will be retained for 6 months from departure date and then deleted unless otherwise instructed.

**Shared Drives**

1. ***Access Controls***

Standard access to the established delivery unit network shared drives is allocated as part of the new starter process. Additional access for other shared drives will be requested by a service request. The request requires authorisation by the Approval Group associated with that network drive.

**Finance & Procurement Systems**

1. ***Overview***

Finance and Procurement systems are used to control and report on finance and manage procurement activities in LBB. The general financial system in use within the authority is Integra; the Income system is Axis and access is provided to authorised users. Roles giving access to transactions are maintained by Finance.

1. ***Control Process***

All access to the finance systems within LBB are controlled by the Finance Approval Group who set up users and allocate business roles within the systems. LBB users requesting access to financial systems must log a service call requesting access which will be forward to the Approval Group for authorisation and action.

The Finance Approval Group will action the request and feedback to the service desk so the call can be appropriately completed.

1. ***Controls Check***

Managers are provided with a report to check the appropriate staff are setup against their cost centre. It is the responsibility of each Cost Centre Manager to ensure that the correct staff have access to their cost centre and report any errors to the Finance Approval Group via a service request for correction.

On leaving the users’ network accounts are disabled. Closure of the network account will suspend access to financial systems.

**HR Systems**

1. **Overview**

TheCAPITA core HR system is used for the administration of Barnet personnel and payroll.

It is administered from the CAPITA location in Belfast and access for LBB employees is granted via an employee portal. The HR system is accessed to check personnel details, book leave and access payslips etc. It is also used by managers to notify new starters/ movers / leavers and to approve tasks via the integrated workflow.

1. **Control Process**

A Barnet manager uses the secure portal to request New Users / Movers and Leavers activities in the HR department HR will check the manager’s authority against the Barnet organisation charts and if the authorisation is correct will action requests in the HR system. When requests are actioned information is issued to ICT via the service desk to enable the New Users / Movers and Leavers process.

Employee access to the portal is granted when a user is set up in the HR system as a Barnet employee. On user setup a onetime password will be allocated which is changed at first use. If a user subsequently requires a password reset for the HR portal. This is achieved by phoning the CAPITA HR Helpdesk desk in Belfast on (9) 0330 606 444. They will then be taken through the security process to enable a new password to be issued.

1. **controls check**

On leaving the users’ network accounts are disabled. Closure of the network account will suspend access to the HR portal.

**Remote Access Provision**

1. **Overview**

Remote access to the LBB network is only allowed from LBB Corporate and Partner corporately owned and managed machines. LBB and partner organisations must when working remotely use two factor authentication (2FA) to facilitate the connection. LBB use RSA tokens for this purpose.

External third parties given access to support applications are required to confirm in writing to the CSG Security Manager that the machines used for access are corporately owned and have current patching and anti-virus in place. The access given when properly authenticated users connect to Barnet systems is the same as those given when working from an office location.

User accounts required for support contractors are only normally made available for the support session so access periods can be controlled. In many cases the 2FA RSA tokens are not given to the support contractor but are held within Capita CSG to further control the ability to access. In these cases the support contractor must dial the CSG ICT infrastructure team to gain access to the token codes required to be able to access the network. This policy can be varied by exception. If there is an agreed need to access systems for support purposes outside normal working hours.

Any directly connecting organization (e.g. a directly connected VPN) must be subject to a CAPITA Network Security Assessment (NSA) carried out by Capita security staff and the users validated against an active directory (AD) entry. Contracts covering the access and purpose of the access must be place before VPN access is granted.

Remote access must be via corporately managed devices. In normal circumstances users should not attempt access from personally owned computers or other personally owned devices which are not specifically authorised. Any such attempt is a breach of the remote access policy.

1. **Controls Process**

Users request the issue of an RSA Token via the service desk with a service request.

**Security Breaches**

Any suspected security breaches, or loss of equipment must be reported immediately to the Service Desk and logged with a service request. If it is suspected that LBB information has been compromised the incident must be reported immediately to LBB’s Information Management Team. Reported security breaches will be investigated in line with the Security Incident Management Policy.

**Reviewed April 2016**