# 10.16 Security Policy

# Policy statement

Information is a key asset for the London Borough of Barnet (“the council”) and its correct handling is vital to the safe and effective delivery of public services. Information is held in physical and electronic ways. Physically held information includes paper copies, files and records etc. Electronically held information includes

information on computers, drives, memory sticks, disks etc.

Any loss of computer systems or the information they contain could have serious repercussions for the council and / or its clients. A breach of security during processing, storage or transfer of data could result in financial loss, personal injury to a member of staff or client, serious inconvenience, embarrassment, or even legal proceedings against the council, and possibly the individuals involved. The International Standard: ISO 27001 Code of Practice defines Information Security as the preservation of three aspects of information:

* + **Confidentiality:** Making sure information is only available to correctly authorised people
	+ **Integrity:** Making sure that the information cannot be corrupted or incorrectly deleted
	+ **Availabilit**y: Making sure that authorised users have access to information etc. when this is required.

In order to ensure the confidentiality, integrity and availability of these systems an appropriate level of security must be achieved and maintained. The council will ensure that the level of security implemented on each of the various systems will be consistent with the designated security classification of the information and the environment in which it operates.

**Core elements for Children Centre Staff**

All children centre staff should adhere to the corporate Information Security 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:

**Physical Security**

* **staff room** – This is for use by staff, volunteers and professional partners. If there are professional visitors to a centre they can use the staff rom if accompanied by a member of staff. The staff room should be secure at all times, especially if it is an area where staff valuables are kept during working hours
* **laptops** – Laptops should be locked away when not in use (end of the day, leaving the centre). They should be kept in a suitable storage cupboard – Laptops can become hot if left on and can pose a fire risk if not stored correctly
* **paper records** – All paper records should be locked at all times unless being used by a member of staff. Paper records should not be left unattended on desks. The security of paper records is the responsibility of all staff, if you notice documents that should be stored securely please act accordingly. Only staff with the approved level of access are permitted to access, view and edit records. Volunteers may have access to records depending on the role they are filling, the volunteer manager and centre manager will complete a risk assessment to determine if a volunteer is able to access records
* **pin numbers** – If doors/premises are secured by an electronic or manual code they should be changed when a member of staff leaves the organisation (this includes agency and volunteers)
* **printers** – All staff should use the network multi-function devises to ensure that the documents they are printing are only released when they are physically present at the device. If the printers are not protected by coded release then it should be situated in a secure location within the centre and staff must collect their printing immediately after sending it to the device.

**Technical Security**

* **laptops** – All laptops should be encrypted. This is in addition to any anti-virus or local login protected on the device. Laptops that are not encrypted should be reported to your IT support for action (laptops that are not encrypted should not be removed from site)
* **desktops** – All desktops should be encrypted. This is in addition to any anti-virus or local login protected on the device. Desktops that are not encrypted should be reported to your IT support for action
* **hand held devices** – All hand held devices should be secured with password entry. All information stored or accessed on a portable device should be done so on a device that is secure and has suitable protection from vulnerability.

**Reviewed April 2016**