Western Health
and Social Care Trust

MANAGEMENT OF USER ACCOUNTS AND PASSWORD POLICY

June 2019

Version 1.4

Western Health
and Social Care Trust

Policy Title	MANAGEMENT OF USER ACCOUNTS AND PASSWORD POLICY
Policy Reference Number	CORP09/009
Original Implementation Date	September 2009
Revised Dates	November 2014 November 2016 June 2019
Approved Date	ICT SMT Approval – 28/03/2019 Finance SMT Approval – 01/04/2019 Trust CMT – 11/04/2019 Staff Side Consultation – 01/05/2019 Trust Board Approval – 13/06/2019
Review Date	2 years after Trust Approval
Responsible Officer	FERGAL DUREY, AD for ICT and Telecommunications

Revised Policy Changes			
Additions:		**Title**	**Comments**
	Section 2, Page 4	Cybersecurity	Inclusion of section specifically related to Cybersecurity. This section will be included in all ICT policies
	Section 4, Page 5	Guidelines for Staff	Password examples Referral to Appendix 1 – HRPTS and PC Logins
	Section 4, Page 6	Mobile and Smart Phones	Advice on locking mobile and smart phones
	Section 5, Page 7	Countermeasures	Inclusion of Content Filtering, Encryption
	Section 5, Page 7	Password Ageing	Explanation and examples
	Section 6, Page 8	Additional Resources	Inclusion of GDPR, FOI, Disposals, ICO, and Data Protection 2018 and other references
	Section 7, Page 9	General ICT Training	Now set out on its own
		E-Learning	Includes sub-section for Cyber Security training. This section is being included in all ICT policies
	Appendices, Page 10	Apendix 1	Password requirements for PC and laptop users logins
		Appendix 2	User Access Request Form
Amendments:			
	Section 1, Page 4	Background and Purpose	Expansion of the who constitutes WHSCT Staff
	Section 4.3, Page 6	Passwords	In general, passwords should be 8 characters minimum and insluce and upper case character
	Section 5, Page 8	Monitoring Removal	Updated Update regarding dormant email accounts and archiving

Table of Contents

1. Background and Purpose

User accounts and passwords are used by the Trust to grant access to information systems and resources. The effective maintenance of these accounts and passwords is a critical part of maintaining our ICT infrastructure and the information it holds.

Given the particularly sensitive nature of the data that Trust employees have access to, there is a legislative requirement on the organisation (and its staff) to employ, promote and adhere to standards that will safeguard patient / client data against unauthorised access.

The purpose of this policy is to establish the rules for the creation, monitoring, control and removal of user accounts. It applies equally to all staff with access to the Trust network, the HSC wide area network (WAN) and any of the clinical or corporate systems that reside thereon.

The measures outlined in this policy will not be effective without the cooperation of all WHSCT staff. These include full-time, part-time, 3rd party consultants contracted by the Trust to work on specific projects, agency and temporary employees including students and volunteers. The cooperation of all such staff, and acceptance of this policy, is therefore a prerequisite to approval for ICT device use.

2. Cybersecurity

Trust staff need to be aware of the risks and potential for loss of data, equipment or embezzlement of funds via Cyberattacks.

*A **cyberattack** is any type of offensive manoeuvre employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys systems or attempts to embezzle users/businesses.*

Cyberattacks can take multiple forms and the following are a few examples;

- Hacking – someone gaining unlawful access to the ICT network, computer, laptop etc and potentially deleting files and/or stealing data.
- Malware – malicious software that can do any number of things e.g. delete files, make systems crash or target communications equipment.
- Ransomware – where a piece of malicious software runs on a PC, laptop or server, and encrypts (garbles) all the data on the device and therefore makes it no longer usable. There is no guarantee that if the guarantee is paid that the device will decrypt or that encryption will reoccur!
  “Wannacry” was an example of a worldwide ransomware (cyber) attack in May 2017

3. Obtaining Access to Systems

Access to Trust systems will be provided upon receipt of a properly completed “User Access Request form” which is available on the Trust Intranet.
(see Appendix 2 for sample)

The set-up and management of email accounts is governed in accordance with guidelines and principles found in the WHSCT *E-mail Policy*.

Under specific circumstances 3rd Party Suppliers may be able to obtain access to the Trust network or systems.

For further details contact the ICT Service Desk -
ICT Department, Altnagelvin Area Hospital, Glenshane Road, Londonderry, BT47 6SB.
Tel: 028 71865124

4. Guidelines for staff

4.1 Account types

The Trust operates 4 levels of account access;

i) Domain/Network User accounts
Standard logon account, for PC’s and laptops, assigned to users
(Password reset every 60 days)

ii) Operational admin account
Accounts with administrative rights on domain pcs, laptops to allow software installation, trouble shooting (limited to ICT Technical support staff)
(Password reset every 60 days. Membership is regularly reviewed)

iii) Domain Admin accounts
Users who have management responsibility for the domain. These accounts have full administrative rights across the entire active directory and membership is tightly controlled.
(Password reset every 60 days . Membership is regularly reviewed)

iv) 3rd party administrative accounts
For the management of application servers belonging to services within the domain. These accounts are limited to administrative rights on the server(s).
(Limited period of access. Membership and access is regularly reviewed)

4.2 General

For certain regionally hosted systems, e.g. HRPTS, Labs, specific personal information is required such as National Insurance Numbers. The provision of this information is a prerequisite to the allocation of a user account.

a) Staff are **NOT** permitted to authorise the creation of accounts and set access privileges for their own use.

b) New accounts will be created with a ‘default’ password that **<u>must</u>** be changed by the account owner upon receipt.
c) Line managers are responsible for ensuring that staff changes which affect system accounts or access are reported immediately to the ICT Department or the respective system manager.
d) ICT Security personnel and respective system managers may be asked to carry out audits of user accounts to ensure appropriate use. User accounts may be suspended at any time as a result of, or pending the outcome of, investigations into suspected abuse or misuse

4.3 Passwords

Passwords are the first line of protection for user accounts and the ‘strength’ of a user’s passwords is key in the Trust’s defence against security breaches.

Trust staff are discouraged from using Trust account passwords for external purposes e.g. registering with external websites.

Screens, keyboards and printers should be appropriately positioned so that they are protected against accidental disclosure of passwords or any other sensitive data.

Passwords should:-

a) **Not** be disclosed or shared. (**<u>No</u>** e-mailing)
b) Not be written down. If it is necessary to write down a password (e.g. for contingency purposes) it should be stored in a sealed envelope in a secure cabinet
c) **Not** attached to any ICT Device
d) Consist of at least one non-alphabetic character
e) Be a minimum of 8 characters, and include an upper case character
f) Be changed at regular intervals if not prompted to do so by a system automatically
g) Be unique for each individual login account
h) **Not** relate to the user or system being accessed
i) Be changed **immediately** on suspicion of any compromise. Such incidents must be reported to the ICT Service Desk

The following are example of poor passwords that **should not** be used;

- “password”
- “passw0rd”
- ABC….
- “12345678”
- “qwerty”

- “star wars”
- Movie or television names
- Seasons
- Football team names
- A person’s name

Certain computer systems, such as HRPTS and PC or Laptop login’s, have a specific requirement. Refer to Appendix 1 for guidelines for a PC or Laptop login.

Note: Use of software for ‘password-cracking’ or any other means of discovering passwords is <u>strictly prohibited</u> and may lead to disciplinary action.

4.4 Mobile and Smart Phones

Owners of Trust mobile and smart phones are to ensure that these devices are protected using either PIN codes or pattern unlock.

Pin codes should:-

a) **Not** be disclosed or shared.
b) **Not** be written down
c) Contain a minimum of 4 digits

Examples of poor pin numbers;

- "0000"
- "1234"
- "2468"
- "7890"

5. Countermeasures

This policy should be seen as one of a number of countermeasures put in place to protect the organisation and its employees from inappropriate access to systems. Additional protection is provided by the following:-

- **Endpoint Security**
  All computers have Endpoint (*anti-Virus* software) installed. The software runs continuously and is updated with the latest version several times a day. Security patches are applied, on a regular basis, to all PC's, servers and laptops that are connected to the Trust network.
  Users of other third party devices/modalities that are attached to the Trust network must make special arrangements to have Endpoint software installed via the ICT Service Desk.
  As part of the Endpoint control measures, certain e-mail attachments are blocked from entering or exiting the HSC network. If an attachment is blocked the user is informed via e-mail of the steps to take to request its release.

- **Encryption**
  The Trust allows the receipt and transmission of encrypted e-mails from/to external organisations. Appropriate encryption mechanisms must be used as approved by the BSO ITS. For more information on how to encrypt e-mails please refer to the procedure listed on the Intranet Website (under ICT, E-mail encryption).

- **Software Updates**
  Some software may contain security vulnerabilities that were not identified prior to its release. These issues can cause programs to run less effectively or make them susceptible to certain malicious software attacks. Depending on the seriousness of the vulnerability, the Trust will distribute updates, known as patches, to all computers connected on the Trust network. Patches will be installed on Trust computers automatically and may require them to restart.

- **Password aging**
  Where systems allow, passwords will be limited to a specific period of use before a forced change e.g.
  PC's and Laptops connected to Trust Network - 60 Days

HRPTS – 90 days
PAS/Patient Centre – 90 Days

- **Monitoring**
  i) The Trust reserves the right to monitor user accounts and may, with appropriate approval, access individual user accounts in the absence of a member of staff.
  ii) Suspected cases of abuse on the system or breaches in policy will be rigorously investigated by ICT, and where necessary, in conjunction with HR staff.

- **Removal**
  i) Access to systems may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected abuse or misuse
  ii) User accounts will be terminated for staff who leave the organisation
  iii) Dormant e-mail accounts, or accounts not otherwise accessed on a regular basis (6 months), will be deemed suitable for suspension. Special leave or periods of extended absence will be taken into consideration.
  These accounts will be continually assessed and *may be* removed at a later date.

6. Additional Resources

This policy should be read in conjunction with other policies relating to effective and appropriate use of ICT services, including

1) WHSCT Internet Policy
2) WHSCT Email Policy
3) WHSCT Server, Desktop and Portable Security Policy
4) WHSCT Malicious Software Policy
5) WHSCT Protocol for the Electronic Transmission of Confidential Information by Fax and Email
6) WHSCT Social Media Policy
7) WHSCT Incident Reporting Policy and Procedures
8) DOH – Code of Practice on Protecting the Confidentiality of Service User Information
9) Information Commissioner – Anonymisation: managing data protection risk – code of practice (www.ico.gov.uk)
10) Information Commissioner – Data sharing code of practice (www.ico.gov.uk)
11) Regulation of Investigatory Powers Act 2000
12) Computer Misuse Act 1990
13) General Data Protection Regulation (GDPR)
14) Data Protection Act 2018
15) Freedom of Information (FOI) Act 2000
16) BSO ICT policies

7. Training

The Trust is committed to staff development and seeks to consistently improve development standards and opportunities for staff in line with organisational objectives, policies and procedures.

7.1 General ICT Training

Should you or your staff require support in the effective use of ICT please contact the ICT Training Team via the ICT Service Desk.

7.2 E-Learning - Cyber Security (as defined in Section 2 of this document)

The Western Health and Social Care Trust have invested in a software solution from Metacompliance Ltd to help ensure that the WHSCT ICT security expectations are understood by Trust staff. This is an E-Learning platform which enables the Trust to push out awareness content to Trust staff. This provides education regarding Cyber Security topics and the importance of Good Practice and Trust policies and thereby protects the organisation from potential attack.

This tool is designed to be intuitive and flexible so that Trust staff can easily register and undertake training at a time and place that suits them.

Note: Lessons learnt from this training, e.g. Phishing emails, can also be applied to the individual’s home environment.

8. Equality & Human Right's Statement

The Western Health & Social Care Trust's Equality and Human Right's statutory obligations have been considered during the development of this policy.

9. Further Information

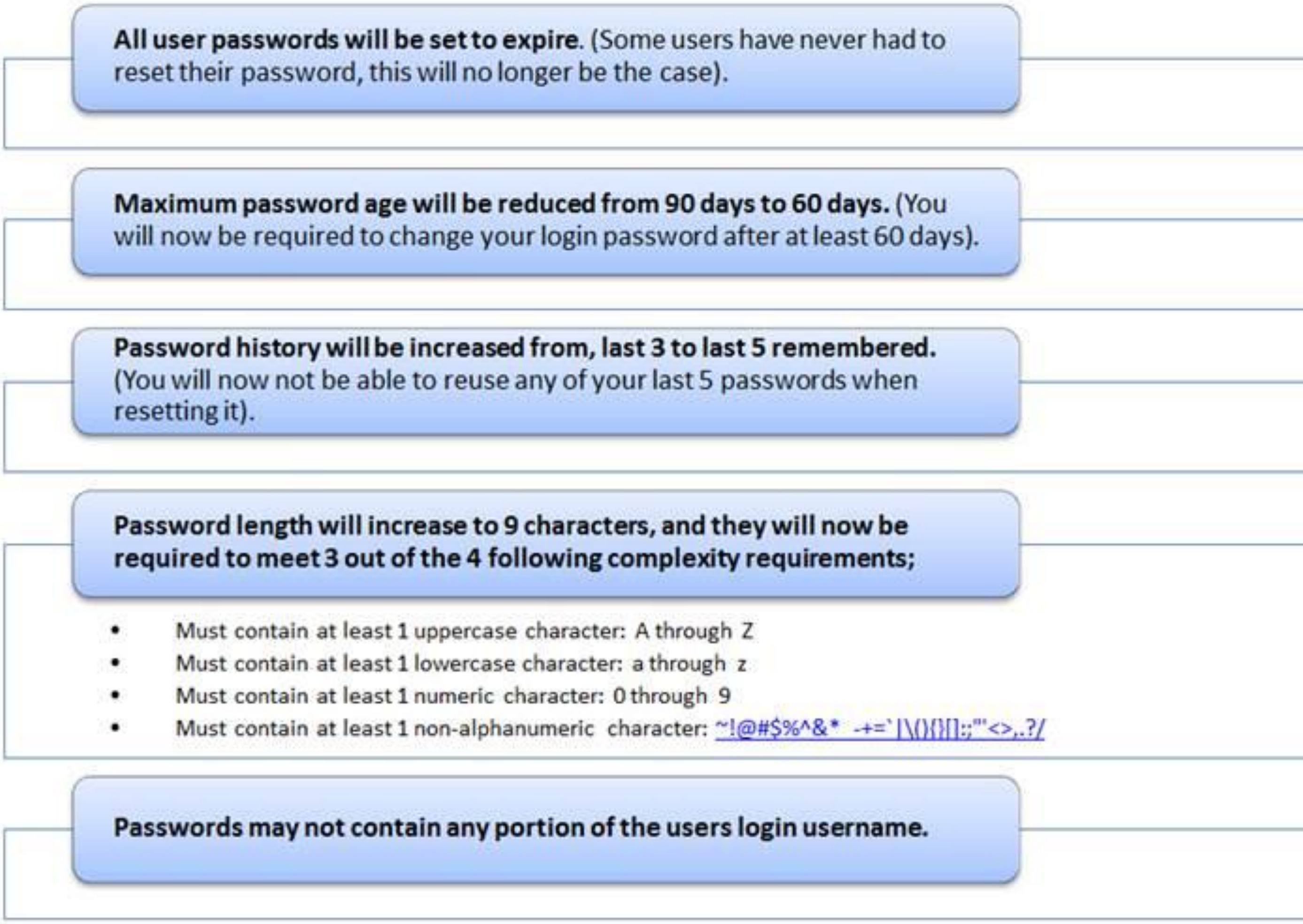
For further information in relation to this policy please refer to:-

The ICT User Forum on the ICT service desk portal available on the Trust intranet link below.

(http://wta-eservicedesk/portal/)

Appendices

Appendix 1- Password requirements for PC and laptop user logins (also known as network or domain login)



All user passwords will be set to expire. (Some users have never had to reset their password, this will no longer be the case).

Maximum password age will be reduced from 90 days to 60 days. (You will now be required to change your login password after at least 60 days).

Password history will be increased from, last 3 to last 5 remembered. (You will now not be able to reuse any of your last 5 passwords when resetting it).

Password length will increase to 9 characters, and they will now be required to meet 3 out of the 4 following complexity requirements;

- Must contain at least 1 uppercase character: A through Z
- Must contain at least 1 lowercase character: a through z
- Must contain at least 1 numeric character: 0 through 9
- Must contain at least 1 non-alphanumeric character: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

Passwords may not contain any portion of the users login username.

Note:- security of the WH&SCT network and data is every employee’s responsibility.

HSC Western Health and Social Care Trust

User Access Request Form

Appendix 2

Requesting Staff (Please complete in CAPITALS)

Name		Job Title	
Department/Ward		Contact No	

Employee Details - ALL FIELDS MANDATORY (Please complete in CAPITALS)

Existing Staff	□	New Staff	□	Proposed Start Date	
Name				Staff No.	
Maiden Name					
Job Title				Grade/Band	
Department/Ward				Contact No.	
Location		PC Asset No.		Shared PC?	□
National Insurance No.					

System Access: (tick all required)

Computer Profile *	□	Outlook Account	□	Webmail Account	□
PAS - Altnagelvin	□	Patient Centre - Altnagelvin	□	LABS – Altnagelvin	□
PAS – TCH / SWAH	□	Patient Centre - TCH / SWAH	□	LABS – SWAH	□
NI Electronic Care Record	□	Flow Bed Management	□	NIPACS	□
DIAMOND	□	Digital Dictation	□	TOMCAT	□
e-Roster	□	TMS	□		
BadgerNet - ALT	□	Twinkle	□	NIMATS - ALT	□
BadgerNet-SWAH	□	Excelicare (Colposcopy)	□	NIMATS - SWAH	□
Child Health System	□	Soscare	□	EPEX CP	□
PARIS	□	PARIS Reports (User/Manager)	□	Epex AMH	□
RMA	□	Comm. Palliative Care	□	Epex LD	□
eNISAT	□	CCS	□	Health & Care Webview	□
Other (Please State)					

Shared Drives (please specify)

Authorisation Details

Line Manager (PLEASE PRINT)			
Job Title		Contact no.	
Signature		Date	

ICT Department Use Only

Service Desk Ref No		Account details	
Forwarded to		Date forwarded	

Completed forms should be returned to ICT Department,
ICT Services Building, Altnagelvin Area Hospital
Glenshane Road, L'Derry, BT47 6SB