APPENDIX 1 - SETTING PASSWORDS (GUIDANCE)

1.0 PURPOSE

1.1 The purpose of this guidance is to enable the maintenance of integrity across the Trust's information systems.

1.2 In line with the ITT Security Procedure it is essential that all Trust staff are aware of their responsibilities to maintain the accuracy, availability and integrity of information held in Trust computer systems.

1.3 The document describes the rules about password maintenance, the standards for the management of access controls in computer based information systems.

2.0 COMPUTER PROTECTION

2.1 Password protection has been used for several years to control access to mainframe computer systems. More recently, passwords have also been implemented in the personal computer and Local Area Network (LAN) environments.

2.2 **What is a password? -** Your computer is your personal key to a computer system. Passwords help to ensure that only authorised individual's access computer systems. Passwords also help to determine accountability for all transactions and other changes made to system resources, including data. If you share a password with a colleague or a friend, you may be giving an unauthorised individual access to the system. What if the individual gives your password to someone else? What if some of your files are deleted or otherwise rendered unusable? Are you willing to take the blame if an unauthorised individual uses your access privileges to damage the information on the system or to make unauthorised changes to data?

2.3 Authentication of individuals as valid users, via the input of a valid password is required to access any shared automated information system. Each user is accountable for the selection, confidentiality and changing of passwords required for authentication purposes. Since you are responsible for picking your own password, it is important to be able to tell the difference between a good password and a bad one. Bad passwords jeopardise the information that they are supposed to protect. Good ones do not.

2.4 Following are some simple rules you should keep in mind about passwords.

- Any system capable of using passwords must have the facility enabled.
- Passwords should be changed frequently. The shorter the life of a password, the better it is. Some systems force users to change their passwords at predetermined intervals.
- Frequency of password change is system dependent and passwords MUST be changed at the frequency appropriate to the system. The default is 30 days for system administrators.
- Passwords should be at least six characters in length. Longer passwords are harder for others to guess.

- Passwords should not be relayed verbally, written down or otherwise revealed to any other individual, either within or outside the Trust.
- Passwords are encrypted (coded) when applied, and therefore cannot be seen by system administrators.
- Never use the same password twice. In fact, good access control systems prevent you from choosing a new password that is the same as your old one. When you are selecting a new password, choose one that is quite different from your previous password.
- Passwords should contain a combination of alphabetic, numeric and special characters (where allowed).
- Avoid using any dictionary words.
- Passwords should not be trivial, predictable or obvious:
    - ***Obvious*** passwords include names of people, pets, relatives, cities, streets, your logon ID, your birth date, car licence plate, and so on.
    - ***Predictable*** passwords include days of the week, months, or a new password that is only one or two characters different from the previous one.
    - ***Trivial*** passwords include common words like ‘secret’, ‘passwords’, ‘computer’, etc.
- Your password should not be the same as your User/Logon ID, an anagram of your User/Logon ID or a palindrome of your User/Login ID. If you have access to a system that require the entry of a password, such as a mainframe computer and a Local Area Network (LAN), try not to use the same password for both systems.
- A good password is relatively easy to remember but hard for somebody else to guess. There are a variety of techniques you can use to choose secure passwords

2.5 The following are examples of these techniques.

1. Use a word with one or two digits embedded in it.
   Examples:

   HOU32SE, MON42DAY, TAB87LE2

2. Make up an acronym based on a nursery rhyme, a favourite song or movie, or a sentence.
   Examples:

   MHALL - **M**ary **H**ad **A** **L**ittle **L**amb; **MDHF#** - **M**y **D**og **H**as **F**leas#; OTGDY - **O**nly **T**he **G**ood **D**ie **Y**oung; **TERM2** - **Term**inator **2**

3. Use a three character pronounceable word suffixed or prefixed with a one- or two-digit suffix or prefix.
   Examples:

   DAM56, WAR34, 56DIG

4. Make up nonsense words that mean something to you by combining the first syllables of two words. However, avoid using standard abbreviations like 'Jan, Feb, Mar, etc.' as part of your password.
   Example:

   PUBPOL - Published **Pol**icy

5. Drop vowels or drop everything but the first 6 letters of a long word or two words.
   Examples:

   CLNDSK1 - **Cl**ea**n D**e**sk, DEDICA5** – **Dedica**tion, **HOMEWO#** - **Home Wo**rk

6. Misspell a word or drop a couple of letters or add some.
   Examples:

   MISTIFI@ - mystify, **CELLEB** – celebrate, **RNYDY$** - rainy day

7. Be creative! And, try to choose a pattern that has meaning for you but that no one else can guess. For example, you might use upcoming events in your life. If you, or one of your children has a major essay to write next month, you might create a password reflecting that event.
   Example:

   MAJESS - Major Essay

8. Or if your 4th cousin, twice removed, is coming for a visit you might create a password such as the following one.
   Example:

   4CUZZ029

9. Another pattern could be to choose meaningful words with a minimum of 10 letters and always use only the first 6 letters. Then add a special character as one of the characters.
   Examples:

   ANNIVE$ - anniversary, **UNBEND#** - unbendable, @**UNBEND** – unbendable, **UN#BEND** – unbendable

10. The best password is one which is a random combination of numeric and alphabetic characters.
    Example:

    48KK439V

***NOTE*: Do not use any of the password examples shown in this document**

11. Finally, please remember that there is no need to share ID's and Passwords. Anyone who needs and qualifies for access to a computer system should submit a request for his / her own Logon ID and password.

2.6 Access to corporate systems will only be given once adequate training has been received and competency levels have been reached, as determined by the trainer / system manager.

3.0 FILE PROTECTION

3.1 Password protection should also be used to protect individual files / documents being transferred across e-mail systems, particularly when passing over person identifiable / sensitive data to external systems / organisations.

3.2 File / document passwords should be applied to all internal transfers of information where it includes person identifiable / sensitive data, as a good practice measure.

3.3 In addition, where regular transfer of such data is required, setting up of shared drives for identified users (i.e. circulation lists for minutes) and giving only appropriately authorised people access would be good / best practice.

4.0 ADDITIONAL GUIDANCE

Refer also to CP9 /CPG9 Records Management Policy / Procedures.
Refer also to CP50/CPG50 Information Governance and Security Policy / Procedures