# APPLY FOR AND SUBSEQUENTLY USE REMOTE ACCESS SOFTWARE PROTOCOL

| Reference No: | UHB 007 | Version No: | UHB 1 | Previous Trust / LHB Ref No: | T/208 |
|---|---|---|---|---|---|

| Documents to read alongside this Policy , Procedure etc (delete as necessary) | Data Protection Policy, IT Security Policy, |
|---|---|

**Classification of document:** IT

**Area for Circulation:** Remote access software users

**Author:** Data Protection Officer

**Executive Lead:** Executive Director of Planning

**Group Consulted Via/ Committee:** IT Security Forum

**Ratified by:** Information Governance Committee

**Date Published:** 13th January 2011

| Version Number | Date of Review | Reviewer Name | Completed Action | Approved By | Date Approved | New Review Date |
|---|---|---|---|---|---|---|
| 1 | May 2010 | Nic Drew | Additional content, and organisational change to UHB | Information & Governance Committee | 29th September 2010 | Jan 2012 |

## Disclaimer

**When using this document please ensure that the version you are using is the most up to date either by checking on the UHB database for any new versions. If the review date has passed please contact the author.**

**OUT OF DATE POLICY DOCUMENTS MUST NOT BE RELIED ON**

CONTENTS Page No.

## 1. Introduction

Software exists to allow users to access and control devices on the UHB's network, thus introducing the risk of inappropriate access to devices. Consequently there is a need for documented conditions of use.

This protocol defines the groups of UHB staff who may use remote access software, explains the application and approval process and sets out acceptable conditions of use.

## 2. Staff groups

There are inherent differences between the following groups of staff that need to use remote access software as a necessary requirement of their job.

### IT Technical Staff

The management of the UHB's network and devices attached to the network requires that appropriate IT technical staff access these devices where such access is necessary. IT technical staff may remotely access devices on the UHB network only when necessary as a part of their duties to maintain the integrity and security of the network and devices or, when as part of their duties they have been invited to do so (e.g. help desk call for assistance).

Not withstanding the Acceptable Use Conditions in section 4, the IT technical staff may, where necessary, use PC-Duo or alternative remote access software to ensure the integrity and security of the network and devices attached to the network.

Where there is a potential risk to the integrity or security of the network or devices attached to the network and it is necessary for IT technical staff to remotely access devices outside the Acceptable Use Conditions; this must be recorded by the relevant line manager.

Only IT technical staff approved by the Head of IT may use remote access software.

### IM&T Security Manager

The IM&T Security Manager conducts investigations into alleged or actual breaches of the UHB's IT Security Policy. Investigations may involve remotely accessing an individuals PC, including files on the PC marked 'Personal', without the individuals consent where informing the individual would compromise the investigation. The IM&T Security Manager will inform the individuals Line Manager and relevant HR Manager of the investigation.

PC-Duo access will be audited; any breaches of this Protocol will be reported to line management and the relevant HR Manager, the result of which may lead to disciplinary action.

**Other IM&T Users**

There are circumstances where other IM&T staff may legitimately require the use of remote access software. All such remote access may only be allowed using remote access software approved by the Information Security Forum (ISF). The remote access software currently approved is PC-Duo and must be used only by specified members of staff for purposes approved by the ISF. All non-IT technical staff using remote access software must sign the Approval Form, appendix 2.

**Non- IM&T Users**

There are exceptional circumstances where non-IM&T staff may legitimately require the use of remote access software. All such remote access may only be allowed using remote access software approved by the Information Security Forum (ISF). The remote access software currently approved is PC-Duo and must be used only by specified members of staff for purposes approved by the ISF.

## 3. Process for non-IT technical staff to use PC-Duo

The procedure to apply for PC-Duo and the approval process are set out below:

**Application**

- The application form (Appendix 1) must be fully completed and returned to the IM&T Security Office
- The application must include written evidence that fully sets out:
  - the proposed user
  - the purpose requiring the use of PC-Duo
  - the explanation as to why the purpose cannot be achieved in any other reasonable way.

**Approval**

The IM&T Security Manager will refer the application to the ISF for approval. The ISF meets bi-monthly. In exceptional circumstances where urgency can be adequately demonstrated, the application may be referred to the Chair of the ISF or the Head of IT for an interim decision.

In considering an application for approval, the ISF will in particular give regard to the following:

- the application clearly demonstrates an unavoidable business need for the use of PC-Duo
- the application clearly demonstrates that PC-Duo is the only realistic solution to the proposed purpose for the use of PC-Duo; i.e. that the same outcome could not be achieved through alternative means
- that the use of PC-Duo by a particular individual or in a particular location would not constitute a risk to the UHB network or devices attached to the network.

## 4. Acceptable use conditions

All remote access software users must comply with the following conditions of use:

- all remote access users must be registered with the IM&T Security Office
- the authorised remote access user will not allow any other person to use remote access
- Files or directories marked 'Personal' must not be accessed without the permission of the file/directory author. ( see IM&T Security Manager conditions)
- Remote access users may remotely access another PC only with that PC users prior consent
- Remote access users may remotely access alter, change or modify content on another PC only with that PC users consent
- Where remote access users need to alter, change or modify software or settings on a PC, they must consult IT technical staff prior to making any changes; unless authorised to do so
- Remote access users must inform staff when they disengage the remote connection
- Remote access users must comply with statutory requirements, e.g. Human Rights Act 1998, Data Protection Act 1998, Computer Misuse Act 1990 and all UHB policies
- Remote access users must be aware of the Duty of Confidentiality they owe others, regarding any personal data they may access.
- It is the responsibility of remote access users to inform the IM&T Security Office when PC-Duo is no longer necessary for their job.

## 5. PC-Duo Administration

- The Data Protection Officer (DPO) will review the Protocol as required, administer the process of applying for PC-Duo use, the removal of PC Duo where necessary and maintain a database of authorised users.
- The PC Duo software will be located in a 'PC Duo Controls User Group' folder on the UHB Domain and accessed using a

Desktop shortcut. Only authorised named individuals in the User Group will be able to access PC Duo.

- Once an application has been approved by the ISF, the DPO will send the applicant's details, to the Help Desk Manager. The Help Desk Manager will arrange for the applicant to be added to the User Group and a shortcut to the Group added to the applicant's desktop.
- IM&T Security Office staff will compare the monthly 'UHB leavers list' against the registered PC-Duo user names. Where a registered user has left the UHB the DPO will inform the Help Desk Manager who will arrange for their name to be removed from the PC Duo Controls User Group.
- Where a registered user changes post but remains in the UHB, PC-Duo access will be removed. The new postholder must apply for and be approved as a PC-Duo user.

## 6. Equality

We have undertaken an Equality Impact Assessment and received feedback on this protocol and the way it operates. We wanted to know of any possible or actual impact that this protocol may have on any groups in respect of gender, race, disability, sexual orientation, Welsh language, religion or belief, transgender, age or other protected characteristics. The assessment found that there was no impact to the equality groups mentioned. Where appropriate we have taken the necessary actions required to minimise any stated impact to ensure that we meet our responsibilities under the equalities legislation.

**APPENDIX 1**

| Ref. No. |
|---|
| |

## APPLICATION FORM TO USE PC-DUO REMOTE ACCESS SOFTWARE

### Purpose requiring the use of PC-Duo

| |
|---|
| |

### Explanation as to why the above purpose cannot be achieved in any other way

| |
|---|
| |

**Declaration**
I agree to abide by the Acceptable Use Conditions detailed in this protocol.

Name…….

Department…….

Signature…….

Date……..

**Line Manager Approval**

Name……..... Signature…….
Date……

**Return form to:**

IM&T Security Office
PSA Building, UHW

**FAX**: 2074 5626
**Enquiries/Assistance**: 2074 6677

| **IM&T Security Office use only** |
|---|
| **ISF Approved** Yes / No **Date**:…… |
| **Reason for non-approva**l: |

**APPENDIX 2**

**APPROVAL FORM TO USE REMOTE ACCESS SOFTWARE**
**IM&T NON TECHNICAL STAFF**

**Declaration:**

- I understand that I may only use remote access software where using the software is a necessary part of my duties.

- I understand that I may not allow any non-authorised person to utilise my remote access privileges.

- I understand that I must comply with the Acceptable use Conditions in the Protocol.

**Name…….. Signature……**

**Date……**

**PLEASE SEND THE COMPLETED FORM TO THE IM&T SECURITY OFFICE, PSA BUILDING, UHW FAX: 2074 5626**