HBL PARTNERSHIP in IT

NHS
Hertfordshire, Bedfordshire and Luton
ICT Shared Services

Mobile Device Security

Document Control

Document Owner	*Keith Fairbrother*	**Approved by**	SMT
Document Author(s)	*Keith Fairbrother*	**Date of Approval**	3/10/2016
Version	*2.0*	**Date for Review**	September 2017

Version Control

Version	Status	Commentary	Date	Author
0.A	Draft	Initial Draft (replacing Policy on use of portable computers and storage devices)	11/2014	K Fairbrother
0.B	Draft	Added restrictions on cloud backup and blocked Apps. Added Appendix 3.	11/2014	M Parsons J Jordan D Muir
0.C	Draft	Various grammatical/spelling changes. Minor sentence changes to improve clarity. Some duplication removed.	14/11/2014	D Muir
1.0	Live	HBL ICT SMT Approval	27/11/2014	HBL ICT SMT
1.1	Live	HBL ICT SMT Approval . Format change	2/10/2015	HBLICT
1.1.1	Draft	Annual review, initial template change	16/8/2016	A McLaren
1.1.2	Draft	Review GC, KF Replace Trust with Partner, update job roles, consistency in ICT Department through document, update Acronyms	23/8/2016	A McLaren
1.1.3	Draft	Update Appendix Devices	27/9/2016	N Ketcher, J Jordan
2.0	Live	Authorized by SMT	3/10/2016	HBLIT SMT

Distribution

Version	Status	Commentary	Date	Author
1.1.2	Draft	**External Action:** None **External Information:** None. **Internal Action:** SMT Review. **Internal Information:** None	8/2016	A McLaren
2.0	Live	**External Action:** Review and authorization from Partners **External Information:** None. **Internal Action:** SMT Review. **Internal Information:** None	9/2016	A McLaren

Implementation Plan

Development and Consultation	With Partner organisations Hertfordshire, Bedfordshire and Luton ICT Shared Services (HBL ICT) is committed to the fair treatment of all, regardless of age, colour, disability, ethnicity, gender, gender reassignment, nationality, race, religion or belief, responsibility for dependents, sexual orientation, trade union membership or non-membership, working patterns or any other personal characteristic This policy / procedure will be implemented consistently regardless of any such factors and all will be treated with dignity and respect. To this end, an equality impact assessment has been completed on this policy.
Dissemination	Staff can access this policy via the Intranet and will be notified of new/ revised versions via the staff briefing. This policy will be included in the CCGs Publication Scheme in compliance with the Freedom of Information Act (FOI) 2000
Training	
Monitoring	*3rd Party Audit, IG Toolkit, spot check*
Review	*The policy will be reviewed annually*
Equality, Diversity and Privacy	

References

External : Legislation, Guidance and Standards	♦
Internal : Related Documentation	♦ Information Security Policy ♦ Guidance on the Use of E-Mail when Sending PCD ♦ E-mail and Internet Policy ♦ Telecommunications Policy ♦ Information Governance Strategy ♦ Information Lifecycle and Management of Records Policy & Procedure ♦ Data Quality Policy ♦ Incident Policy ♦ Confidentiality Policy ♦ Health and Safety at Work and Personal Safety ♦ UK Law with Regard to Usage of Mobile Telephony in Vehicles ♦ Data Protection Act ♦ All applicable UK and EU Laws ♦ CESG Good Practice Guidelines
Enclosures	♦

Contents

Terms and Acronyms

Term	Definition
DH	Department of Health
DVD	Digital Versatile Disc
EU	European Union
HDD	Hard Disk Drive
PCD	Personal Confidential Data
PCs	Personal Computers
SD	Secure Digital
SIRO	Senior Information Risk Owner
SSD	Solid State Drive
USB	Universal Serial Bus

Executive Summary

This policy sets out the Partner's position on the use of Mobile Devices in order to minimise the risks of unauthorised disclosure, modification, removal or destruction of the Partner's information assets.

The term 'mobile device' includes but is not limited to the following:

- Mobile computer devices including:
  - Laptops/Ultrabook
  - Tablets
  - Smartphones
  - Wearable Technology
  - Any other 'mobile' computer device which has the potential to store Personal Confidential Data (PCD).
- Mobile Storage devices including:
  - Digital Cameras
  - Digital Dictaphones
  - SD Cards
  - External USB devices (stick)
  - External Hard Disk Drives
  - Any other externally connected device which has the potential to store Personal Confidential Data (PCD).

Mobile Computer/Storage Devices issued to staff by the organisation and in their possession are the property of the Partner. Equipment is supplied for official Partner business and must not be used for any personal purpose.

Requirements are stricter than for office-located devices because of the much greater risk of loss or damage to the Partner's information and property.

Any mobile device issued by the Partner to any member of its staff must only be used in accordance with the organisation's policies and procedures. Failure to comply with the Partner's policies and procedures or to comply with the guidance in this document could result in disciplinary action and legal proceedings.

Application of the policy will assist in compliance with the Partner's Information Security Policy, information related legislation, NHS Information Security Standards and NHS Information Governance Standards

1 Introduction

- The Partner is an organisation committed to ensuring that diversity, equality and human rights are valued. We will not discriminate either directly or indirectly and will not tolerate harassment or victimisation in relation to gender, marital status (including civil Partnership), gender reassignment, disability, race, age, sexual orientation, religion or belief, trade union membership, status as a fixed-term or part-time worker, socio-economic status and pregnancy or maternity.

- The Partner works to a framework for handling personal information in a confidential and secure manner to meet ethical and quality standards. This enables National Health Service organisations in England and individuals working within them to ensure personal information is dealt with legally, securely, effectively and efficiently to deliver the best possible care to patients and clients.
- The Partner via the Information Governance Toolkit provides the means by which the NHS and Partner can assess our compliance with current legislation, Government and National guidance.
- Information Governance covers:
  - Data Protection & IT Security (including smart cards),
  - Human Rights Act,
  - Caldecott Principles,
  - Common Law Duty of Confidentiality,
  - Freedom of Information Regulations and
  - Information Quality Assurance.

2 Scope

This policy covers but is not limited to:

- All Mobile Computer/Storage Devices that are in use on any information system owned or operated by the Partner
- Any Mobile Computer/Storage Device used to store or process any information belonging to the Partner

Examples of Mobile Computer/Storage Devices include:

- Laptop/Ultrabook (HP, Lenovo, Toshiba, Dell)
- Tablets (Apple iPad, Samsung Galaxy Tab, Microsoft Surface Pro)
- Smartphones (Apple iPhone, BlackBerry, Windows Phone, Amazon Kindle)
- Wearable Technology
- Digital Cameras
- Digital Dictaphones
- External Memory devices (SD Card)
- External USB devices (Stick, HDD)
- External Hard Disk Drives (SSD, iPod, MP3 Player)
- Magnetic Storage:
  - Cassette Tape
  - Floppy Disk
- Optical Storage:
  - Compact Disc (CD)
  - MiniDisc (MD)
  - Digital Versatile Disc (DVD)
  - High Definition DVD (HD DVD)
  - Blu-ray Disc (BD)

All other permutations will need written approval from the ICT Department Head of Technical Services and Partner's SIRO/IG Lead. For example: an external training provider/consultant who requires access to a Partner computer to deliver training material/presentations by use of an external USB device.

For a comprehensive list of supported Mobile Computer/Storage Devices see Appendix or the ICT Department, HBLICT Intranet page.

3 Responsibilities

3.1 Authority for Use

- Each business unit will identify its business requirements for the use of Mobile Computer/Storage Devices and the number of devices needed to satisfy those requirements. These requirements will be reviewed periodically.
- Mobile Computer/Storage Devices must only be used when there is a clear and documented business requirement that has been approved at the appropriate level within the Partnership (see Appendix). The use of removable media by subcontractors or temporary workers must be risk assessed and be specifically authorised.
- Staff and contractors must not use any Mobile Computer/Storage Device that has not been provided by, or explicitly approved by, the Partner. Approved devices will be appropriately identified and a central register of devices issued will be maintained. A local register of devices in use must also be maintained.
- Mobile Computer/Storage Devices will be supplied (and/or approved) by the ICT Department when requested by the responsible authority level within the Partner (Appendix) and when there is no suitable alternative method of meeting the business requirement.
- All bulk data extracts and transfers of person-identifiable or other confidential information using a Mobile Computer/Storage Device must be authorised by the Partner's SIRO/IG Lead who must also ensure that a record is maintained of all such extracts and transfers.
- The Partner's Caldicott Guardian must also approve bulk extracts and transfers containing person-identifiable information relating to patients.
- The security level and configuration of Mobile Computer/Storage Devices will be specified by the ICT Department's Head of Technical Services in consultation with the Partner's Information Governance Manager and will be installed, configured and maintained by the ICT Department.
- The use of any Mobile Computer/Storage Devices may be restricted or blocked if the ICT Department's Head of Technical Services or the Partner's Information Governance Manager considers:
  - They create an unnecessary risk to the Partner's information assets.
  - There is a breach, or potential breach, of the Partner's Policies or the NHS Information Governance Standards.
- Managers will be responsible for the day-to-day management and oversight of Mobile Computer/Storage Devices used within their work areas to ensure the Partner's policies and guidance are followed. This will include:

- Ensuring devices that have not been allocated or are not currently in use are stored securely.
- Maintaining a record of Mobile Computer/Storage Devices within their area of responsibility, the staff who have been authorised to use them and the devices allocated to those staff. For example: asset number, device, employee name, storage location and date of allocation.
- Ensuring that devices are only used for the purposes and business requirements for which they were supplied.

- Members of staff who have been authorised to use Mobile Computer/Storage Devices for the purposes of their job roles are responsible for the secure use of those removable media as required by the Partner's policies and guidance.

3.2 Security and Care

- Only authorised and approved Mobile Computer/Storage Devices can be used within the organisation. Requests for additional devices must be made in writing to the ICT Department's Head of Technical Services and the Partner's IG Manager for review and approval.
- PCD must not be stored on any device that is not approved for this purpose. Approved devices will have additional safeguards to protect their contents and will be clearly marked.
- Mobile Computer/Storage Devices must only be used to store, transfer and share NHS information for the agreed business purpose. When that business purpose has been satisfied the devices must be returned for re-use or recycling as appropriate.
- The information on Mobile Computer/Storage Devices must be a copy of information that is held securely elsewhere. These devices must not be used to hold the only, or the primary, copy of information.
- A record must be kept of the data on each Mobile Computer/Storage Device. The devices must be physically protected against their loss, damage, abuse or misuse when in use, when stored and when in transit.
  - Devices should be stored appropriately (e.g. in the protective case supplied for laptops, tablets and smartphones, etc.) when not in use.
  - In public places, computers and protective cases should be as understated as possible. Smaller devices (smartphones, etc.) should be located securely in another bag or in an inside pocket.
  - Ensure devices are handled carefully to avoid being dropped or damaged in any way. Protect from direct sunlight, excess heat and moisture/rain.
  - Where relevant, any security locks or alarms supplied must be attached and activated when devices are unattended.
  - Any unattended device, even in your own home, should be secured against unauthorised access.
  - Devices must not be left in cars or any other location where there is a risk of theft or damage.
  - Peripherals and accessories provided by the Partner must not be used on any other device or computer. Only peripherals and accessories supplied by the Partner may be used on Partner issued devices whilst they are connected to the network.

- Do not allow any unauthorised person to use a Partner issued device; this includes patients/service users, family and friends.

- All incidents involving theft or malicious damage of a Mobile Computer/Storage Device must be notified to the ICT Department's Service Desk immediately. The police must be notified if the incident occurred away from Partner premises. On Partner premises, the senior or site manager must be informed. The Finance Department must be notified in accordance with the Losses and Compensation procedures documented in Partner Standing Financial Instructions.
- All incidents involving the use, loss or damage of any Mobile Computer/Storage Device must be reported immediately in accordance with the Partner's incident reporting procedures.

3.3 Mobile Computer Devices

The device will be configured for the purpose it is to be used and all the necessary software will be installed. Any changes to the configuration and/or installation of additional software will be performed by the ICT Department. Requests should be made through the ICT Department's Service Desk. **Do not** attempt to make any changes yourself.

- Keep your Usernames and Passwords secure:
  - Passwords must be a mixture of letters and numbers at least eight (8) characters long.
  - Do not use your name, names of family or pets as a password.
  - Change your password frequently: every 60 days or less.
  - Never tick the 'Remember Password' box when logging-in.
  - Do not write down usernames and/or passwords.
  - Do not enter username and/or password when you can be overlooked.
  - Do not give your username/password to anyone else.

You must safeguard all information on the Mobile Computer Device from loss, damage, corruption and unauthorised access or disclosure.

- Backup the data on the Mobile Computer Device regularly to the network.
- Keep back-up copies of data safely and separately from the Mobile Computer Device.
- Do not use the Mobile Computer Device in a public place where the screen can be observed.
- Do not use unapproved cloud based backup, storage or data sharing solutions (see Appendix).

You must have the express permission from your Department Manager or other Partner authority (see Appendix) to store or process any confidential or sensitive information on the Mobile Computer Device, particularly if this is personal data about patients, staff, etc.

You must also have the express permission of the Caldicott Guardian if any of the personal data relates to Service Users or Clients. Any conditions as to the scope and content of the information and to time periods must be strictly observed.

All Mobile Computer Devices that may be used to store or process personal data must have special data encryption software installed. This will either be supplied with the

computer or can be installed retrospectively by the ICT Department. Please contact the ICT Department's Service Desk accordingly.

Tablet and Smartphone devices that will be used to access Partner resources (e-mail, Intranet, documents) must be provisioned with an appropriate Mobile Device Management platform. This is to ensure that the appropriate level of security is active to comply with the necessary CESG and IG regulations.

Some Mobile Computer Devices are used as a shared resource amongst a group of staff. Where this happens there must be a clear and up-to-date record of who is the current holder of the device.

Any unauthorised person must not use Mobile Computer Devices. These are principally people not employed by the Partner: patients, family, friends etc., but may include colleagues particularly if they are not part of the same workgroup or they should not have access to sensitive or confidential information on the Mobile Computer Device.

The Mobile Computer Device will be supplied with virus protection software installed. Virus protection must remain active at all times and not disabled, bypassed or removed.

Members of staff are responsible for ensuring that security software (Anti-Virus, Anti-Malware, Firewall and Operating System updates) is maintained and kept up-to-date. Most Mobile Computer Devices will update automatically when connected to the Partner's network. Staff must connect their Mobile Computer Device to the Partner network at least once a month to update the security software in addition to exercising vigilance and good practice to keep the Mobile Computer Device free of malicious software. In particular:

- Check regularly for security updates to Windows (Tools/Windows Update in Internet Explorer).
- Do not open suspicious e-mails and do not open attachments to e-mails you don't recognise.
- Do not download programs or executable files from the Internet; this includes screen savers.
- Remote access using Strong Authentication can be arranged if you need to use the Partner's network services, such as e-mail, when you are away from the office. This will also provide remote Internet access. Requests for remote access should be made by completing the appropriate forms available from the ICT Portal or via the ICT Departrment's Service Desk. Instructions for the use of Strong Authentication will be supplied as part of the installation process.
- Mobile Computer Devices must not be connected to broadband or Internet services unless you have been authorised and issued with the appropriate Strong Authentication token. The connection must be made using the network cable provided or via a wireless connection which utilises WPA2 encryption as a minimum security standard.
- Connections must not be made to public or proprietary wireless networks (this includes but not limited to Internet cafes and public Wi-Fi hotspots). It is strictly forbidden to connect to the Internet or other online services except through the Strong Authentication service provided or unless given written permission to do so by an approved authority (Appendix).

4 Requests for New Devices

All requests for Mobile Computer/Storage Devices should be made to the ICT Department's Service Desk.

Requests for Mobile Storage Devices must be supported by a business requirement with the appropriate level of authorisation (see Appendix). Devices will not be issued until the ICT Department's Head of Technical Services and/or the Partner's IG Manager has approved the request.

Devices will be issued to a named individual who will be responsible for its safekeeping and appropriate use. All devices that can be encrypted or password protected will be issued with the protection already in place. Instructions for use will be supplied.

All Mobile Computer/Storage Devices will be tagged and must be made available whenever a reasonable request is made to inspect or audit the device.

Appendix A. Supported Mobile Computer/Storage Devices

The list below is the current supported environment at the point of writing. Due to the rapid development of technology and devices, this list is liable to change. For an updated list of available and supported devices please refer to the ICT Intranet.

1. Laptop/Ultra Book Devices

Supported HP Devices (Laptop/Ultrabook)	Supported OS
EliteBook 2570p EliteBook 820 G1 EliteBook 840 G1 EliteBook 840 G2 EliteBook 840 G3	(SA: Software Assurance) Windows 7 Enterprise (inc. SA) 32-bit/64-bit
ProBook 6570b ProBook 650 G1 ProBook 650 G2	Windows 7 Enterprise (inc. SA) 32-bit/64-bit
Supported Toshiba Devices (Laptop/Ultrabook)	**Supported OS**
Tecra R940 Tecra R950 Tecra A50-A-151 Tecra A50-A-18M	Windows 7 Enterprise (inc. SA) 32-bit
Portege Z10T-A-103 Portege Z10T-A-12J	Windows 8 Professional 64-bit or Windows 8.1 Professional 64-bit
Supported Dell Devices (Laptop/Ultrabook)	**Supported OS**
E6420 E6430 E6440 E7450	Windows 7 Enterprise (inc. SA) 32-bit or Windows 7 Enterprise (inc. SA) 64-bit
Supported Panasonic Devices (Laptop/Ultrabook)	**Supported OS**
none	none
Supported Lenovo Devices (Laptop/Ultrabook)	**Supported OS**
Twist N3C27UK	Windows 8 Professional 64-bit or Windows 8.1 Professional 64-bit

2. Tablets

Supported Apple iPads	Supported iOS
iPad (1st Generation)	5.1.1
iPad 2 iPad (3rd Generation) iPad (4th Generation) iPad Air iPad Air 2 iPad Mini iPad Mini 2 iPad Mini 3	8.0, 8.1,9.0,9.1,10.0,10.01 ***Plus subsequent versions of iOS as advised by ICT Department***

3. Smart Phones

Supported Apple iPhones	Supported iOS
iPhone 5 iPhone 5c iPhone 5s iPhone 6 iPhone 6 Plus	8.0, 8.1, 9.0,9.1,10.0,10.1 **Plus subsequent versions of iOS as advised by ICT Department**
Supported Samsung Android Phones	**Supported OS**
Samsung J3 and J5	
Supported Windows Phones	**Supported OS**
Nokia (Microsoft) Lumia: 635, 640, 650	8.1, 10.1

WindowsPhone (smart Phone will no longer be supported and produced by Microsoft). Wearable Technology

4. Wearable Technology

- tbc

5. Digital Cameras

- Canon
- Flip Video Camcorder (Flip Video Camcorder USB Device)

6. Digital Dictaphones

- Olympus DS 7000 voice recorder
- Olympus Digital Dictator (OLYMPUS DVR USB Device)
- Olympus Digital Dictator (OLYMPUS DVR DM SERIES USB Device)

7. External Memory Drives

- SD Cards for use in Digital Cameras and Digital Dictaphones

8. External USB Devices

- Integral Courier (Integral Courier TL USB Device)
- Integral Courier (Integral Courier FIPS 197 USB Device)
- Integral Courier (Integral Crypto USB Device)
- Kingston Data Traveller (Kingston DTVault Privacy USB Device)
- Kingston Data Traveller (Kingston DTVaultPrivacy30 USB Device)
- diskGenie (diskGenie USB Device)
- MXI (MXI Private USB Device)
- SafeStick (BM SafeStick BE USB Device)
- SafeXS (Ctwo SafeXs USB Device)
- SanDisk (SanDisk Enterprise USB Device)
- SanDisk (SanDisk Enterprise FIPS USB Device)
- O2 Mobile Broadband Dongle (ZTE MMC Storage USB Device)
- O2 Mobile Broadband Dongle (CWID USB SCSI CD-ROM USB Device)
- One Touch Mobile Broadband Dongle (ONETOUCH SUZUKA USB Device)
- One Touch Mobile Broadband Dongle (ZTE MMC USB Device)
- Thera Trainer (USB2.0 Flash Disk USB Device)
- RBA HCC RAS (USB Flash Disk USB Device)
- RBA HCC RAS (SMI USB DISK USB Device)

9. External Hard Disk Drives (SSD, iPod, MP3 Player)

- Western Digital My Passport Drives (Additional Authorisation Required)

Appendix B. Authority Levels

The list below is the approved authority levels as described within the policy.

- Director
- Assistant Director
- Associate Director
- General Manager
- Locality Manager
- Head of Service
- SIRO
- Caldicott Guardian
- IG Manager

Appendix C. Prohibited Mobile Device Applications

The list below is not exhaustive but highlights common apps that have been risk assessed by the Partner's IG teams and therefore should not be installed on corporate devices or used for the transfer, backup, sharing or distribution of Partner information. For an updated list of prohibited applications please refer to the HBL ICT Intranet.

- Cloud Storage:
  - Apple iCloud
  - Microsoft OneDrive
  - Dropbox
  - Google Drive
  - Box
  - SpiderOak
- File Sharing:
  - Tappin
  - Office 365
- Collaboration Tools:
  - Huddle
  - Evernote

Appendix D. Equalities Impact Assessment Stage 1 - Screening

1. Policy		**EIA Completion Details**
Title: Information Security Policy		Names & Titles of staff involved in completing the EIA:
☐ Proposed ☐ Existing	Date of Completion:	
Review Date:		

2. Details of the Policy. Who is likely to be affected by this policy?		
☐ Staff	☐ Patients	☐ Public

3. Impact on Groups	**Probable impact on group?**			**High, Medium or Low**	**Please explain your answers**
	Positive	**Adverse**	**None**		
Race, ethnicity, nationality, language etc.	☐	☐	☐		
Gender (inc. transgender)	☐	☐	☐		
Disability, inc. learning difficulties, physical disability, sensory impairment etc.	☐	☐	☐		
Sexual Orientation	☐	☐	☐		
Religion or belief	☐	☐	☐		
Human Rights	☐	☐	☐		
Age	☐	☐	☐		
Other:	☐	☐	☐		
No impact on any of the groups above.	Explain and provide evidence that policy applies equally to all staff				

4. Which equality legislative Act applies to the policy?	
☐ Human Rights Act 1998	☐ Age Equality Regulations 2006
☐ Sex Discrimination Act	☐ Equal Pay Act
☐ Race Relations Act	☐ Sexual Orientation Regulations 2003
☐ Disability Discrimination Act	☐ Religion or Belief Regulations 2003
☐ Gender Recognition Act 2004	☐ Health & Safety Regulations
☐ Mental Health Act 1983	☐ Part time Employees Regulations
☐ Equality Act 2006	☐ Civil Partnership Act 2004
☐ Mental Capacity Act 2005	

5. How could the identified adverse effects be minimised or eradicated?

6. How is the effect of the policy on different Impact Groups going to be monitored?

Appendix E. Privacy Impact Assessment Stage 1 - Screening

1. Policy	**PIA Completion Details**
Title: Information Security Policy ☐ Proposed ☐ Existing Review Date:	Names & Titles of staff involved in completing the PIA: Date of Completion:

2. Details of the Policy. Who is likely to be affected by this policy?		
☐Staff	☐ Patients	☐ Public

	Yes	**No**	**Please explain your answers**
Technology Does the policy apply new or additional information technologies that have the potential for privacy intrusion? (*Example: use of smartcards*)	☐	☐	Application of the policy will minimise potential for privacy intrusion.
Identity By adhering to the policy content does it involve the use or re-use of existing identifiers, intrusive identification or authentication? (*Example: digital signatures, presentation of identity documents, biometrics etc.)*	☐	☐	Application of the policy will ensure integrity of information.
By adhering to the policy content is there a risk of denying anonymity and de-identification or converting previously anonymous or de-identified data into identifiable formats?	☐	☐	Application of the policy will ensure integrity of information.
Multiple Organisations Does the policy affect multiple organisations? (*Example: joint working initiatives with other government departments or private sector organisations*)	☐	☐	Policy applies to organisation only. All other NHS organisations have similar policy based on the same standards.
Data By adhering to the policy is there likelihood that the data handling processes are changed? *(Example: this would include a more intensive processing of data than that which was originally expected)*	☐	☐	Application of the policy will ensure integrity of information during processing.

2. Details of the Policy. Who is likely to be affected by this policy?	
If Yes to any of the above have the risks been assessed, can they be evidenced, has the policy content and its implications been understood and approved by the department?	

Appendix F. Comment Form

As part of HBL ICT Services Department continuous improvement regime, would you please complete this form. Any comments or feedback on this document should be addressed to the Owner. Please provide your name and contact details in case clarification is required.

Name .....

Address .....

.....

Phone .....

Email .....

Please return to:

HBL ICT Services

Charter House

Welwyn Garden City

Hertfordshire, AL8 6JL

Please confirm the document you want to give response to as:

HBL ICT Business Continuity Plan

Please rate the document using the topics and criteria indicated below:

	Very Good	Good	Average	Fair	Poor
Format and Layout					
Accuracy					
Clarity					
Illustrations (tables, figures etc.)					

When using the document, what were you looking for?

.....

How could the document be improved?

.....

How often do you use the document?

.....

If you have additional comments, please include them below:

.....

.....

Thank you for your time