



Birmingham City Council

Flexible and Remote Access Standard

If you have inquiries about this Standard,
Contact the Intelligent Client Function on 0121 675 1431 or 0121 464 2877.

Standard ***Gerry McMullan – Business Policy Manager***
Owner: ***Birmingham City Council***
Author: ***Mrs M A Westrop – Information Security
Manager***
Version: V3
Date: 03102008

© Birmingham City Council 2008



Produced in conjunction with

1. OVERVIEW AND PUBLICATION PARTICULARS	3
2. PURPOSE OF THE FLEXIBLE AND REMOTE ACCESS STANDARD	6
Scope	6
3. STANDARD PARTICULARS	7
3.1 Arrangements before Access is Granted	7
3.1.1. Conditions to be met before Remote or Flexible Access is Granted to Staff	7
3.1.2. Conditions to be met before Remote or Flexible Access is Granted to Third Parties	9
3.2 Rules to be obeyed during Remote and/or Flexible Access.....	10
6. ENFORCEMENT	14
6. APPENDIX I.....	15
Manager’s Check List - only approve Remote or Flexible Access if all sections are ticked. 15	
6. APPENDIX II the Authorization Form.....	17

1. OVERVIEW AND PUBLICATION PARTICULARS

Document History (Old format)

Version	Date	Notes
1.0	October 2004	Out for QA – Steve Fear
1.0	October 2004	Second QA – Nigel Jones, Craig Price
1.1	November 2004	Draft for Approval
Draft 1.2	June 2005	Revised due to Anywhere Computing Project
Draft 1.3	July 2005	Updated following consultation
Draft 1.4	July 2005	Updated following further consultation
Draft 1.5	February 2006	Updated prior to presentation to CISG
Draft 1.6	February 2006	Updated post presentation to CISG
Draft 1.7	March 2006	Updated post meeting with DPA Section
Final Draft	April 2006	For CISG group approval
Final Draft 1.9	October 2006	Update to reflect organisational changes.
Final 2.0	November 2006	Update following feedback from Focus Group
Final 2.1	November 2006	Update for Wireless controls
2.2	220808	Update document names, PSPG database and information classifications Nigel Jones

Document History (New format)

Version Amendment	Date	Purpose	Author
2.3	280808	Re-write following new Risk Assessment	MW
2.4	110908	Changes after ICF comments	MW
2.5	180908	ICF changes to tick list at end	MW
2.6	180908	Changes from Alan Keepax,	MW
2.7	25092008	Changes from Jill Walker	MW
2.8	02122008	ICF, Terry Holsey, Andrea Baker, Paul Hartles, Craig Price. Particularly now the ICF want the form introduced – see Appendix II.	MW sitting with DT and CH
2.9	03102008	Typographical errors and fixes	MW

Document Distribution after approval

Version	Name	Organisation
3.0	PSPG	Birmingham City Council

Document Reviewers

Version Amendment	Date	Name & Organisation
2.2 risk assessment and 2.6 draft	8 th August & 18 th Sept	Andy Pyper (Link to ICT), Moh Zaheer (SB Technical Design Unit), Caroline Hobbs (BCC Intelligent Client Function), Louise Milner (Audit), Gordon Bunce (Network Services), Jaspal Sagoo (Technical Security Manager SB), Terry Holsey (SB Project Manager Working for the Future), Varun Shingari (BCC Legal), Raymond Holmes (Local Services), Madeleine Westrop (Security and Policy Manager SB); Russell Waldron and John Owen SB Security (Deputised to Jaspal Sagoo), David Thomas (ICF), Andrea Baker (Education), Craig Price (deputised to Louise Milner), Vicky Murray (Local Services, deputised to Raymond Holmes), Philip Wilson (Social Services) Balgit Kundi (SB Working for the Future), Dave Hall (SB Telecommunications).
2.5	11 th and 18 th Sept	CISG , Terry Holsey, Paul Hartles, Craig Price
2.6	25 th Sept	Lynden Smith, Sajid Rehman, Sandra Mackenzie, Service Desk

Document Approval by Birmingham City Council

Version	Date	Name	Role	Signature
2.9	15102008	BTAG		

Overview

Authority ^a	Birmingham City Council – Head of Policy & Co-ordination
Owner ^b	Birmingham City Council – Business Policy Manager
Scope ^c	See introduction below
Review period ^d	This document should be reviewed at least annually, or more often if there is change of circumstances.
Related Birmingham City Council documents	Information Security Policy; Internet Use Policy; Internet Use Code of Practice; Access Control Standard; Information Security Classification Standard; Disposal of Information Processing Standard; Information Asset Management; Data Protection Policy; Internet Monitoring Standard; Records Management Policy; Password; Ten Email Security Principles for Elected Members; Malicious Software Standard; Incident Response Standard.

^a AUTHORITY: The person or organisation who is responsible for enforcing this Standard.

^b OWNER: The organisational position of the person who has rights to authorise changes to, or disposal of this Standard

^c SCOPE: The organisations or persons to whom the Standard applies.

^d REVIEW PERIOD: How frequently the Standard should be reviewed.

<p>BS ISO/IEC 27001:2005</p> <p>BS 7799-2:2005</p> <p>control references</p>	<p>Control Reference</p> <ul style="list-style-type: none"> A.7 Asset Management <ul style="list-style-type: none"> A.7.1.3 Acceptable use of Assets A.7.2 Information Classification <ul style="list-style-type: none"> A.7.2.2 Information Labelling & Handling A.8.3.3 Removal of Access Rights A.9.1.1.Physical security perimeters A.9.2.1 Equipment siting and protection A.9.2.5 Security of Equipment off-premises A.9.2.7 Removal of Property A.10.1.3 Segregation of Duties A.10.8.1 Information exchange policies and procedures A.10.8.3 Physical media in transit A.11.1.1 Access control policy A.11.2.2 Privilege management A.11.3.2 Unattended user equipment A.11.3.3 Clear desk and clear screen policy A.15 Compliance with legal requirements <ul style="list-style-type: none"> A 15.1.1 Identification of applicable legislation <ul style="list-style-type: none"> A.15.1.3 Protection of organizational records.
--	--

2. PURPOSE OF THE FLEXIBLE AND REMOTE ACCESS STANDARD

If a person obtains Remote Access or Flexible Access to information owned or controlled by Birmingham City Council they must follow the rules in this Standard.

A person has “Remote Access” when they are authorized to process this information from a position outside the Council’s networks. For example, the Council has contracts with external parties which allows them Remote Access to view and handle data at their own premises; some staff may get permission to work from home using a dedicated telephone line^e to connect their computer at home to the Council’s network.

A person has “Flexible Access” when they are authorized to use such information at a variety of locations either within, or outside, the Council network. For example, staff or contractors may not have a permanent desk but instead might carry a laptop computer on which they access the Council’s email or other systems from diverse offices, hospitals, courtrooms, planes and trains.

The data handled and transmitted after Remote and Flexible Access is set up, is more vulnerable to accidental corruption or deliberate modification, loss or inappropriate disclosure than data processed at a permanent desk within a Birmingham City Council office.

Birmingham City Council requires all those within the scope of this Standard to follow the rules in the Standard in order to protect the confidentiality, integrity and availability of City Council information. This is particularly important in view of the “Enabling Agile Working” programme.

Scope

This Standard applies to all electronic information^f processed either by Birmingham City Council, or processed on behalf of the Council by a third party, regardless of the ownership of the devices or electronic networks used to process that information. The Standard also applies to all electronic information owned by Birmingham City Council^g.

The obligations outlined in this Standard apply to all employees, agency staff, elected members (or other public representatives), trustees, third parties under a contract, employees of associated organisations or volunteers.

This Standard applies wherever the work is done, anywhere in the world: for example at home, office or in transit or from a remote site.

^e Frequently, where the City has paid for an ‘ADSL’ telephone line to someone’s house.

^f Data is processed whenever information is indexed, classified, stored, recorded, disseminated, published, copied, organised, amended, retrieved, viewed, disclosed to others, deleted, destroyed, transferred, transmitted, declassified: *it is difficult to say there is any activity directed towards the data, which does not amount to processing.*

^g For rules about handling hard-copies and non-digital information generally, see the Handling and Labelling Standard and the records management policies.

3. STANDARD PARTICULARS

3.1 Arrangements before Access is Granted

3.1.1. Conditions to be met before Remote or Flexible Access is Granted to Staff

An “Authorizing Manager”^h must authorize all Remote and Flexible Access. They can only allow this access after a list of tests have been successfully passed: these are set out in the Manager’s Check Listⁱ and every test must be ticked. In particular, note:

1. Remote or Flexible Access can only be granted if the Manager has established that this is beneficial for conducting the business of Birmingham City Council.
2. The Manager must make it understood that, when Birmingham City Council owned equipment is allocated to staff for Remote or Flexible Access, it can be used only by specified members of Birmingham City Council staff and not by their families, friends or associates or unauthorized business colleagues.
3. Remote Access for staff is only permitted if the staff member and their Manager have completed a Risk Assessment and have found this sort of access is appropriate for the remote locations. The Manager must be satisfied that risks are justified and all available precautions are in place. Additionally, the staff member who works flexibly from many locations must assess risk for each new location.

The risk assessment must include consideration of the information security classification^j. *Remote and Flexible Access is not appropriate for the use of Restricted information* and should only be used if for this sort of information if it is absolutely necessary. If such access to Restricted information is authorized by the Manager, extra security must be used, which would include, wherever possible, encryption^k.

4. Managers must only permit Remote or Flexible Access for staff if they are confident that the staff being given such access know and understand this Standard and all relevant security policies^l and the Data Protection Act rules. Managers must give copies of the relevant policies to the staff concerned and a signed Authorization Form^m should be kept by the authorizing manager and a copy should be kept by the member of staff concerned. Audit may demand sight of these Authorization Forms at any time from either party.

^h An “Authorizing Manager” in this document is the Birmingham City Council line manager for staff using remote or flexible access; or the Birmingham City Council or Service Birmingham contract manager for contractors, consultants, or partners using remote or flexible access; or the Birmingham City Council manager responsible for others such as Elected Members or volunteers who are authorized to use Remote or Flexible Access. If Authorizing Managers move they should allocate the responsibility to their replacement. If this is not done, responsibility passes to their own manager.

ⁱ For [Managers’ Check List](#), see end of document.

^j Rules are set out in the Classification Standard and the Labelling and Handling Standard and Code of Practice.

^k See also the Labelling and Handling Standard and Code of Practice regarding two factor security .

^l See [related documents](#), above.

^m The [Authorization Form](#) is attached at the bottom of this document.

5. All access must be arranged through the Service Birmingham Service Deskⁿ who will manage the process of making the connections and establishing the access privilege permissions.
6. A remote or flexible worker can only use their own equipment for this access only if
 - a) the Authorizing Manager puts in writing their Assyst request to Service Birmingham, what type of connection and what software is going to be used; and Service Birmingham must only make the connection if they then approve
 - i. That the speed and capacity of the connection is sufficient and secure;
 - ii. And that the specification of the Client^o Software to handle the electronic connection with the Council's network is trusted;
 - And b) Authorizing Manager first agrees with the Applicant for that access that the Applicant will keep his
 - iii. Anti-virus protection will be kept up-to-date;
 - iv. Firewall^p access security, content filter, anti-virus and security barrier protection is sufficient and up-to-date;
 - v. Operating System^q Service Pack^r specification will be kept up-to-date;
 - vi. Client^s Software on their equipment used to handle the electronic connection with the Council's network licensed;
7. The Manager must take appropriate technical and security advice to check that the software applications on the remote or flexible worker's computer are appropriate for the Security Classification of the data being processed^t.

ⁿ Telephone 464 4444 or complete the Service Desk Request form: use this form to specify the requirement in 6a).

^o "Client" software operates on the remote or flexible users' equipment. These remote or flexible users use this Client software to request information exchange with the City's "Server" computers. For example, programmes such as Internet Explorer that display and interact with Internet sites are part of the Client software.

^p A "Firewall" is a security application or security device which controls network traffic to and from a computer. It either permits or denies communications traffic.

^q The "Operating System" is the computer programme that manages all the other programmes and shares the resources on a computer.

^r The Operating System "Service Pack" is the computer programme code that has been written to correct, fix and update the operating system when it is installed into the existing Operating System.

^s "Client" software operates on the remote or flexible users' equipment. These remote or flexible users use this Client software to request information exchange with the City's "Server" computers. For example, programmes such as Internet Explorer that display and interact with Internet sites are part of the Client software.

^t Contact Business Policy by e-mail or on 464-2877 and refer to the Information Security Classification Standard.

3.1.2. Conditions to be met before Remote or Flexible Access is Granted to Third Parties

1. Where persons are authorized to connect remotely to Council information, a Birmingham City Council or Service Birmingham Manager (the “Authorizing Manager”^u) must in every case be responsible for the security of the connection.
2. This Authorizing Manager must monitor the Remote Access and must make sure that the third party is accountable to that Manager for their use of Council equipment, resources, systems and information.
3. The Authorizing Manager must agree with the Third Party in writing:
 - i. That the speed and capacity of the connection is sufficient;
 - ii. That anti-virus and anti-spyware protection will be kept up-to-date;
 - iii. That Firewall access security, content filter, anti-virus and security barrier protection is sufficient and will be kept up-to-date;
 - iv. The specification of the Client Software to handle the electronic connection with the Council’s network is trusted and licensed;
 - v. That the Operating System Service Pack specification will be kept up-to-date;
 - vi. Where and how the equipment can be connected to the network.

A copy of this agreement must be kept by the Authorizing Manager and may be required for inspection by Audit at any time.

4. The Authorizing Manager must take appropriate technical advice to make sure that the software applications on the remote or flexible third party’s computer are appropriate for the Security Classification of the data being processed.
5. The Manager is responsible for making sure that suitable contractual provision is made for the security of data, return of data, prohibiting the copying or unauthorised transfer of data^v, for insurance, licensing, copyright, encryption and confidentiality.
6. The Authorizing Manager is responsible for making sure that the third party knows the Classification, Handling and Labelling, Password, Access, Internet, Email, Monitoring, Data Protection and other BCC Security Policies, Standards and Codes.
7. Furthermore, the Authorizing Manager must tell the third party the correct procedure for reporting all data loss or accidental data disclosure.
8. Authorizing Managers must also make sure that any connections are disabled and all data is returned, once the contractual period ends. Authorizing Managers must inform Service Birmingham when third party access arrangements are ended.

^u See also the Authorizing Manager for employees in section 3.1.1. above, and the application form in [Appendix II](#) below.

^v Note that this means that City Council data stored on a disk or other portable memory device, should not be copied to the local memory of any equipment without permission; and that at the end of the processing, all temporary or log files with copies of the processed data must have their contents be deleted.

3.2 Rules to be obeyed during Remote and/or Flexible Access

1. The Use of publicly available equipment and communications

a) All those connecting remotely must take all reasonable steps to identify who is providing the equipment and connections used and to ascertain that they are a reputable provider. For example, workers should not use hotel-provided Internet connections unless they approve of the reputation of the business^w.

b) No public access service advertised as free in the street or public places can be used for corporate business.

2. Flexible Access location risk assessment

a) All workers or contractors must assess potential security risks *before* starting to work in each new or public location.

b) During use, information must be viewed or otherwise processed privately and the user must log out if they leave the machine^x.

3. Remote Access is exclusively for Business Use

Remote Access is allowed for business use only. Staff and contractors may not use Remote Access for private purposes. For example, staff are not permitted to connect remotely to the corporate network from their laptop on the train, if they are connecting in order to do personal shopping on the Internet.

The Council does allow some private use of BCC equipment and systems but this is a privilege only and generally limited to workers who use BCC equipment from within BCC-owned or BCC-controlled premises. Any other personal use of BCC equipment needs to be authorised specifically by an appropriate manager.

4. Remote Connections can be made Through, but never directly To, the Internet.

a) BCC-owned equipment may be permitted to connect remotely into the Council's corporate networks through the Internet if:

i) The connection is made through software approved and provided by Service Birmingham;

ii) The connection is encrypted;

iii) Security Policies are followed;

iv) All 'ad hoc' networking capabilities are switched off (for example, there should be no access to free or costed public Internet access);

v) There is no simultaneous connectivity to public access networks (except where the public access networks are controlled by Service Birmingham or Link2ICT).

^w And for technical advice, contact Service Birmingham Security Team 0121 303 4743.

^x See the Handling and Labelling Code of Practice sections on Use and Physical Security.

b) The connection across the Internet is only permitted directly into the Council and nowhere else. BCC owned equipment must *never* be connected directly to other sites on the Internet through an independent Internet Service Provider.

c) If a remote or flexible worker or contractor requires business access to the Internet, they must first connect into the Council networks and only then connect out of the Council and into the Internet through the Council's Secure Gateway.

5. Possession and use of BCC equipment

a) Council owned equipment may only be used remotely or flexibly by specifically authorized staff or contractors. All Council equipment is controlled within a business area. Authorizing Managers in a business area must know and control exactly who can use equipment assigned to their business area. For example, if staff take BCC-owned computers or routers home, or out of BCC premises for mobile working, the equipment must not be used by their family members.

b) Council owned equipment should not be left unattended in public places; portable computers should be carried as hand luggage and disguised where possible when travelling. Manufacturers' instructions for protecting equipment should be followed: for example protect equipment from exposure to strong electromagnetic fields or temperature extremes. *It is the responsibility of the person who is given Council Equipment or data to guard it, to check advice from Service Birmingham or the manufacturer and to anticipate difficulties and judge the best way to keep the data and equipment securely.*

c) As stipulated by the Software Control Standard, only the Service Birmingham Service Desk are allowed to install software on BCC equipment.

d) Service Birmingham should approve hardware and other equipment before it is connected to BCC equipment. Contact Service Birmingham for security advice on whether equipment is approved. Memory sticks or CDs from unknown or distrusted sources should never be connected to BCC equipment. If memory devices are found but not identified, they should not be put into equipment but should be sent to Service Birmingham Security for investigation.

e) Remote and Flexible workers must not use BCC equipment if they find devices or software on that equipment which they do not recognize and trust. They should immediately report any such concerns as Security Incidents to the Service Birmingham Service Desk.

f) Equipment is controlled by a team within the corporate structure and can be allocated to the team members for Remote or Flexible Access by an Authorizing Manager for that team. As soon as the team members leave or move jobs, they must return equipment to the appropriate team. If the business reason for the remote or flexible access has expired, then the equipment must be returned to the appropriate team.

6. The Use of non-BCC equipment for Remote or Flexible Access

a) Remote and Flexible workers must check equipment before use for any unexplained devices or software. They must not use equipment if attached devices or software are

not recognized or not trusted. They should not connect such equipment to the Council's networks or equipment. They should immediately report any such concerns to their Corporate Information Security Group representative. For example, equipment with key-logging devices, or installed with key-logging software, always poses a very serious and unacceptable security risk.

b) No Internet connections may be made or authorized from remote locations into the Council from non-Council equipment through encrypted "VPN"^y routes (virtual private networks). This is because these connections can be controlled by hackers who then enter the Council network and can do much damage.

d) After each use of non-BCC equipment for remote access to the Council networks, all logs and caches and other private data must be cleared and deleted wherever this is possible^z.

e) Contractors and business partners who work flexibly must obey the rules for Third Party Remote Access ([above](#)).

f) Contractors who work flexibly must not connect their own equipment or memory devices to the Council's network unless the contract Manager has first agreed the conditions set out in 3.1.2. [above](#).

7. Loss, Accidental Disclosure and other Security Incidents

Security incidents^{aa} must be reported immediately to the appropriate management and to BCC Security on 0121 440 4743 who will log the incident and report it to the ICF. Contractors, third parties and all within the [scope](#) of this document must also do this.

Loss or theft of equipment or information must also be reported to the UK Police and a crime reporting reference should be noted for the security breach record.

^y "VPN" is an encrypted computer network connection through the Internet.

^z The method for this varies with each operating system, the way the system is 'locked down' by the administrator of the system and the internet browser. For example, in Internet Explorer, if you can, click on Tools, Internet Options and then the General. Then click on Delete Cookies, Delete Files and Clear History.

^{aa} For a definition of a security incident, see the Incident Response Standard on the PSPG database.

ROLES AND RESPONSIBILITIES

Role	Organisation	Responsibility
<p>Employees, agency staff, elected members or other public representatives, trustees, third parties under a contract, employees of associated organisations or volunteers within the Scope (qv) of this standard.</p>	<p>All within Scope</p>	<p>To follow the rules of this Standard as set out above & BCC Security Policies and Standards;</p> <p>To report all loss of equipment or information and all security breaches or accidental disclosure of information to BCC Security on 303 4743 or through the Service Desk 4 4444.</p> <p>To report all thefts of equipment to Council Management, BCC Security through the Service Desk and to the Police.</p>
<p>Corporate Management Team</p>	<p>Birmingham City Council</p>	<p>To manage and maintain controls which keep information secure as required in this Standard.</p>
<p>Intelligent Client Function – Business Policy Manager</p>	<p>Birmingham City Council</p>	<p>To make sure the Information Flexible and Remote Standard meets business needs and is reviewed annually as a minimum. To respond to reports of lost or compromised data or equipment, or security breaches, to assist the CISG (Corporate Information Security Group).</p>
<p>Birmingham City Council Managers</p>	<p>Birmingham City Council; Service Birmingham on behalf of Birmingham City Council.</p>	<p>A line manager or contract manager, (“Authorizing Manager”), must authorize all Remote and Flexible Access only after the tests in the Manager’s Check List have been successfully passed and the application form has been signed by the applicant;</p> <p>An Authorizing Manager must be confident that the technical standards have been reached if non-BCC equipment is used (see 3.1.1 (6) and 3.1.1(3));</p> <p>Authorizing Managers must remain responsible for flexible and remote access which they have permitted as long as they stay in the job role and, if they leave or move without arranging a new Authorizing Manager, the responsibility then rests with their own manager.</p> <p>Managers must communicate this Standard and related policy and guidelines to all staff and third parties connecting remotely or flexibly;</p> <p>Management who are responsible for third party contracts are also responsible for the security of data and connections made by that third party to the City Council’s networks. They are also responsible for the security of Council data processed by that third party. These duties and others are set out in section 3.1.2. above.</p> <p>Management must report security issues and anomalies resulting from Remote or Flexible Access to the Corporate Management Team and to Strategy, Policy and Business Security.</p> <p>Management must know and control the use of</p>

		<p>all equipment and information within their business area.</p> <p>CISG representatives must assess reports of unexplained devices or software and may need to report these on to Business Security.</p>
Network Services and Service Desk	Service Birmingham	<p>To provide, manage and maintain equipment, software and connections to the Council network which meet the Service Birmingham security standards and are kept up to date;</p> <p>To make sure all Internet connections are encrypted and are made through approved software, install client connection software and keep records of what connections are made and who authorized them;</p> <p>To configure Council owned equipment so that independent internet access is denied and ad hoc networking options are turned off;</p> <p>To advise and agree by email or in writing with Council Management what technical standards are required, particularly for non-BCC equipment connected to the Council's networks: (see 3.1.1 (6a) and (7));</p> <p>Not to connect equipment to the Council's information systems unless the connection is authorized by a Manager; and must not connect equipment which is not owned by the Council through 'VPN' connections to the Council's systems.</p>
Service Birmingham Business Security Team		<p>To log lost or compromised data or equipment and report it to the ICF.</p> <p>To log and assess unexplained software or devices reported through the CISG representatives.</p>

6. ENFORCEMENT

Any member of staff who contravenes this Standard may be investigated under the City Council's disciplinary procedure and, where appropriate, legal action will be taken.

Third parties, partners and other individuals within the scope^{bb} of this Standard, who contravene its terms, may have their right to handle City Council information revoked and may jeopardise their relationship with Birmingham City Council. They may also face legal action.

^{bb} See [Scope](#), above.

^{bb} In line with ISO27001:2005 A 10.8.1

6. APPENDIX I

Manager's Check List - only approve Remote or Flexible Access if all sections are ticked.

Check	Tick
<p>Risk Assessment: confirm the value of Remote or Flexible working outweighs the information security risks? Particularly consider:</p> <ul style="list-style-type: none"> - the classification of information and the risks and effect of its accidental disclosure, loss or corruption, - how private or public and what associates will be nearby, - what precautions there are against infection by Malicious Software^{cc}, - how vulnerable the arrangement would be to hacking attacks^{dd}, - costs and efficiency of Remote or Flexible working. 	
Are you satisfied this access is the most appropriate and cost effective way of working?	
Have you considered the sensitivity and Security Classification of the data to be accessed? ^{ee}	
Has Data Protection training been provided to all staff working remotely or flexibly?	
Is the remote or flexible worker or contractor aware that no information can be disclosed, copied, transmitted, deleted or collected without the appropriate authority and security precautions (See the Handling and Labelling Standard and Code of Practice)?	
Where staff are concerned, have they received training on how to use the equipment?	
Have Health & Safety issues been assessed and addressed?	
Have all remote or flexible workers or contractors read and understood this Flexible & Remote Access Standard?	
Will all workers or contractors understand that they must assess potential security risks <i>before</i> starting to work in each new or public location?	
Are there arrangements to keep anti-virus software, firewalls and operating systems up to date?	
Does the remote or flexible worker or contractor agree to return any equipment given to them by the Council when leaving the council or moving or changing their employment or contract?	
Does the remote or flexible worker or contractor agree Has to report the theft or other loss of any equipment used to Management, Service Desk and Police where appropriate?	
Is the applicant aware that support, insurance and maintenance is only available for BCC equipment?	
Is the remote or flexible worker aware that any connection to their own Internet Service Provider from BCC-owned equipment (including PCs and routers) is NOT permitted?	

^{cc} See the Birmingham City Council Malicious Software Standard.

^{dd} Advice on this is available from BCC Security 303 4743

^{ee} See the Information Security Classification Standard and the Handling and Labelling Standard and Code of Practice for more information.

Has the Authorizing Manager has agreed in writing the following specifications with Service Birmingham for all third party connections:

- i. The speed and capacity of the connection
- ii. Anti-virus and anti-spyware protection which is kept up-to-date
- iii. "Firewall" access security, content filter, anti-virus and security barrier protection
- iv. The specification of the 'Client' Software to handle the electronic connection with the Council's network
- v. The 'Operating system service pack' specification: that is, the software used to run the system on any remote device should be up to date
- vi. That the software applications are appropriate for the Security Classification of the data being processed.
- vii. Where and how connections are permitted?

6. APPENDIX II the Authorization Form

Request for Remote or Flexible Access

This form should be completed by any Applicant within the scope of the Flexible and Remote Access Standard who is requesting Flexible or Remote Access as defined in this Standard.

The applicant should keep one copy of the signed form; the Authorizing Manager should keep another copy of the form. These forms must be shown to Birmingham City Council Audit upon demand.

Applicant: Please complete all sections in block capitals

Information recorded on this form and any reports, recommendations and correspondence arising from this information will be processed by Birmingham City Council and Service Birmingham in accordance with the Data Protection Act 1998 and all relevant legislation.

Name	Network Identity when you log onto the BCC Network, if you have one
<input type="text"/>	<input type="text"/>
Telephone Number	Email address
<input type="text"/>	<input type="text"/>
EMPLOYEES:	
Employer	Job Title
<input type="text"/>	<input type="text"/>
Division of Birmingham City Council if appropriate	Directorate in Birmingham City Council if appropriate
<input type="text"/>	<input type="text"/>
NON-EMPLOYEES: In what capacity are you acting when you have Flexible or Remote Access (e.g., are you an elected Member, Volunteer, Work Experience assistance, self employed or acting in another capacity)	
<input type="text"/>	

I have received a copy of the City Council's Flexible and Remote Access Standard attached to this form, including the section on Enforcement and I have received the [related standards, policies and codes of practice](#), which I have read and understood. I agree to abide by all the standards, policies and codes of practice. I realize that the council's security software may record any information I transmit or receive.

Print Name.....

Signature..... Date.....

Authorizing Manager Please complete all sections in block capitals. Authorizing Managers must be employees of Birmingham City Council or Service Birmingham.

Authorizing Manager's Name	Manager's Network Identity when you log onto the BCC Network, if you have one	
Authorizing Manager's Telephone Number	Authorizing Manager's Email address	
Employer (Birmingham City Council or Service Birmingham)	Job Title	
Division of Birmingham City Council if appropriate	Directorate in Birmingham City Council if appropriate	
Assyst Reference Number:	Budget Code :	Cost assessment details:
Business Reason for request:		
Type, sensitivity and Information Security Classification of data which will be accessed:		

I authorize support the Applicant's request for Remote or Flexible Access to the BCC Network and take responsibility for all my duties under this Standard. I confirm that the Applicant has been made aware of BCC security Policies, Standards and Codes.

Print Name

Signature..... Date.....