Information Sharing Agreement: Newcastle Gateway (v.1.5)

Name of Agencies:

Gateway Referral Agencies:

National Probation Service
Northumbria Community Rehabilitation Company Limited
Northumberland Tyne and Wear NHS Foundation Trust

Gateway Service Providers:

Action Foundation
Changing Lives
Crisis Skylight Newcastle
Depaul UK
Gateshead Housing Company (Rough Sleeper Social Impact Bond delivery partner)
Haven (Tyneside) Limited
Home Group Limited
Karbon Homes Limited
Keyring Living Support Networks
Mental Health Concern
Mental Health Matters
Newcastle City Council
Newcastle Futures Limited
North of England Refugee Service
Phoenix Futures
Places for People
Praxis Service
Richmond Fellowship
Shelter North East
St. Vincent de Paul Society
The Albert Kennedy Trust
Thirteen Group
Tyne Housing Association Ltd
Your Homes Newcastle

Gateway Support Partners (Supporting Independence Scheme)

Action for Children
Advocacy Centre North
Affinity Sutton Homes
Barnardo's Pause Newcastle Project
Bernicia Homes
Byker Community Trust
Change Grow Live (CGL)
Newcastle Carers Centre
The Guinness Partnership
Two Castles Housing Association

Subject to change based on service demands – signatories will be notified of any additions

In respect of:
Newcastle Gateway

Effective From: 5 September 2011
Latest revision: 31 May 2017

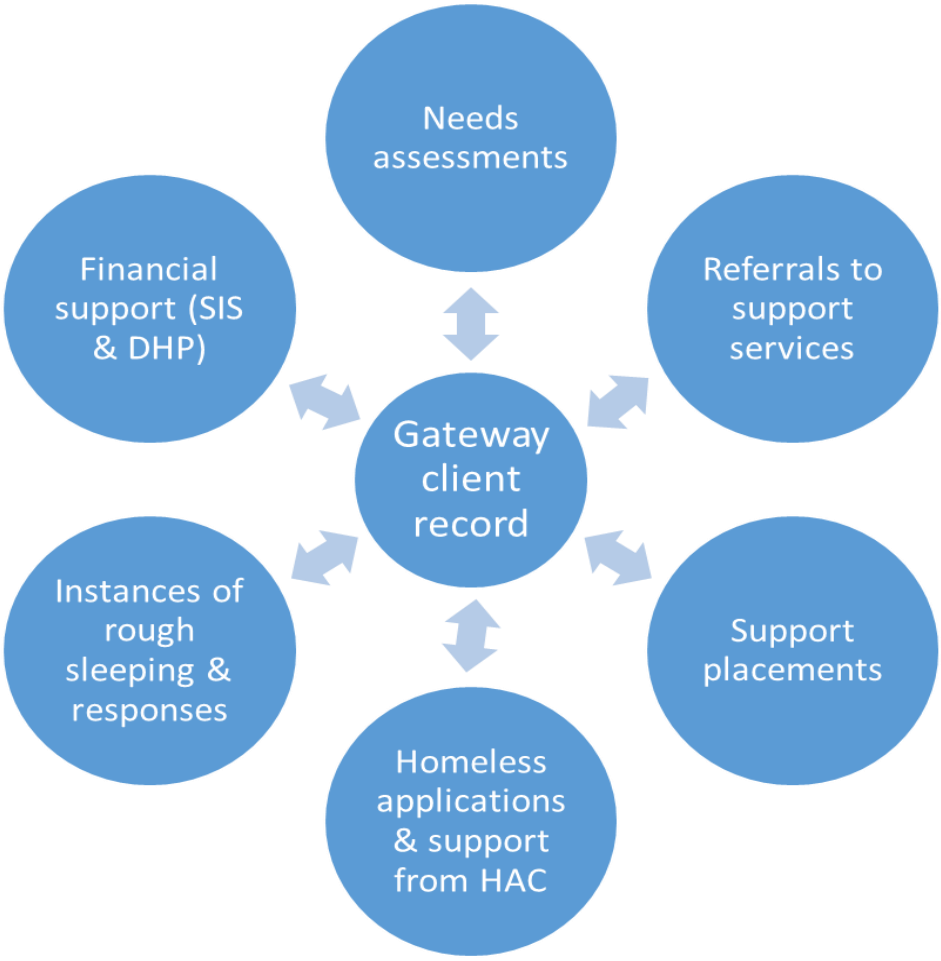
1. OPERATIONAL REQUIREMENTS

1.1 Target (Service User) Group

Newcastle Gateway manages referrals to and details of placements with statutory temporary accommodation, supported accommodation, housing-related support services and employment support services, benefits and debt advice services, and applications for financial support through the Supporting Independence Scheme (SIS) – part of Newcastle's local welfare provision. Clients who are involved with a partner agency listed above may be referred to these services via Newcastle Gateway. The Gateway also holds details of residents who have applied for Discretionary Housing Payments (DHP) and require referral to additional support, Your Homes Newcastle (YHN) tenants where YHN have commenced eviction proceedings, clients who have been found rough sleeping and/or are supported by the Council's Multiple Exclusion Common Case Management Group (MECCMG), and clients seeking advice from the Housing Advice Centre.

Not all Gateway users will have access to all data about all client; access to client records and client or service information is restricted to relevant users, by means of user category restrictions and individually configured permissions.

1.2 What is to be shared?



Newcastle Gateway allows partner agencies within the city to share details of clients seeking the support described above with providers of these services, via a secure web-based system. This will include sensitive personal data about clients' current and historical housing, relationships, support needs and support workers involved, financial situation, risks to others or themselves, ethnic origin, religious beliefs, sexual orientation, where relevant to the service being sought. Depending on the support needs and circumstances of the client, their Gateway client record may contain details of:

- Household composition, support needs and involved support agencies, risks, housing history and pertinent financial information e.g. arrears, debts, income, and employment
- Referrals made to Gateway support services, responses, support placement duration and outcomes
- Homeless applications, outcomes and advice provided by the Housing Advice Centre, including calls to the Emergency Homeless Officer (EHO) line
- Instances of rough sleeping, as verified by outreach workers, and records of clients monitored via MECCMG
- Applications to and awards from the Supporting Independence Scheme (SIS)
- Applications to DHP support, details of awards and referrals to additional support to meet needs identified
- YHN eviction proceedings

Not all Gateway users will have access to all data about all clients; access to client records and client or service information is restricted to relevant users, by means of user category restrictions and individually configured permissions.

1.3 Purpose of Information Sharing

The purpose of sharing information is to carry out statutory homelessness duties, match individuals with available housing, financial inclusion and employment support, ensure these services are targeted at the most vulnerable groups to prevent homelessness and financial exclusion, monitor the performance of commissioned services, identify and respond to trends in homelessness and financial inclusion including identifying opportunities for earlier intervention, and to develop services to better meet the needs of clients seeking support.

The purposes of information sharing via Gateway are to create a single record for each client requiring or receiving support from the services above to ensure continuity of support and sharing of essential risk information with partners from whom that individual may require support.

Additionally, Newcastle Gateway collects aggregated data which will be used to:

- Monitor performance of commissioned services against contractual aims and inform the commissioning process
- Monitor patterns and trends in service use, reasons for seeking support (such as causes of homelessness) and outcomes achieved (such as number of homelessness preventions) to develop a citywide consensus and response
- Complete statutory returns to government

1.4 Legal Basis for Information Sharing

There is legal provision which permits this information sharing, described below.

Data Protection Act 1998: permits sharing with data subject consent. The Data Protection Directive on which the UK's Data Protection Act is based defines 'the data subject's consent' as: 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'. The Data Protection Act also permits sharing, without explicit consent, where necessary for exercising statutory functions, monitoring equality of opportunity, or where sharing is necessary to protect the individual's "vital interests".

Crime and Disorder Act 1998: permits sharing where information exchange is necessary to prevent crime or disorder. This may include details of geographical restrictions on a client; risks posed to individuals in temporary or supported accommodation or to certain groups e.g. children.

Housing Acts: permit sharing where information is necessary to impose an injunction or eviction, or to uphold a tenancy. This may include details of relevant incidents, cautions or convictions known to the Police.

2. SERVICE USER IMPACT ASSESSMENT

2.1 Privacy and Confidentiality

Sharing of the information described via Newcastle Gateway is necessary to gain access to services, enable support providers to make informed allocation decisions, monitor equality of opportunity and to carry out statutory homelessness advice functions. Partners will inform clients which services have been identified as appropriate for their needs and allow them to identify any service/s that they do not wish their information to be shared with.

Signatories to this agreement will be required to maintain client confidentiality by protecting client information from disclosure to third parties or unnecessary disclosure to other agencies. Providers also agree to securely destroy any hard copies of client data after use.

Each signatory agency will take responsibility for their compliance with data protection legislation and this agreement; Newcastle City Council will provide guidance on these issues where concerns arise. The Information Commissioner's Office Data Sharing Code of Practice may also provide useful guidance.

Partners are expected to publicise this agreement to all staff who have access to Newcastle Gateway and to investigate any reports of poor practice or breaches of the agreement by their staff. Partner agencies are responsible for ensuring the information they upload to Newcastle Gateway is accurate and relevant; once information is uploaded to Newcastle Gateway, Newcastle City Council will assume the role of "data processor" with responsibility for maintaining the online system and processing requests for data subjects' access to personal data in compliance with the Data Protection Act. Reported breaches of this agreement will be investigated by

Newcastle City Council and, if deemed necessary by Newcastle City Council, access withdrawn from the individual/s or agency involved.

2.2 Service User Consent

Service users will be required to consent to their information being shared as a prerequisite to applying for support via the Newcastle Gateway. It should be explained to clients that by giving their consent to their details being shared via Gateway that they are agreeing to all relevant information being shared with Newcastle City Council and support providers, including any relevant information not disclosed at the time of the assessment. This may include convictions, charges, cautions or recorded incidents related to arrestable offences, breaches of tenancy or licence agreements, or illegal / immoral use of the property, provided one of the disclosure conditions of Schedules 2 and 3 of the Data Protection Act 1998 apply.

Client consent may be recorded on a standard consent form provided by Newcastle City Council. This will be retained by the referral agency and referrals should not be made without a signed consent form, unless this is considered as being in the client's "vital interests".

If a client withdraws their consent for their information to be shared via the Newcastle Gateway, the referral agent will alert the Active Inclusion Newcastle Unit (AINU) who will delete their client record. Service providers who have received a referral from that client will be informed and will then securely destroy any hard copies of client details they may have.

If a referrer identifies any safeguarding or welfare concerns and consent cannot be obtained or is refused from a client who you believe to be vulnerable and/or at risk of serious harm and in need of support, you may still make referrals to support services without their consent. However, in accordance with Data Protection Act principles, you must document the reasons for your decision on the client record. For advice on individual clients in this position, Gateway operators should contact the AINU in the first instance.

Consent should be sought at the point of registration onto the Gateway and at the point of referral. The client should be reminded of their right to withdraw consent at any time, and that refusal to share their details will limit the support that can be offered to them.

2.3 Service User Awareness and Rights

Clients will be made aware of the purpose and context of this Agreement, its impact upon them, their rights and how these may be exercised via the client consent form and through verbal or additional written explanation by partner agencies.

In the event of a complaint being received by any signatory organisation about the use or disclosure of personal data or information, all relevant partners must be advised as soon as possible and in any event within seven calendar days. Each agency will deal with complaints in accordance with their own procedures, the results of which will be

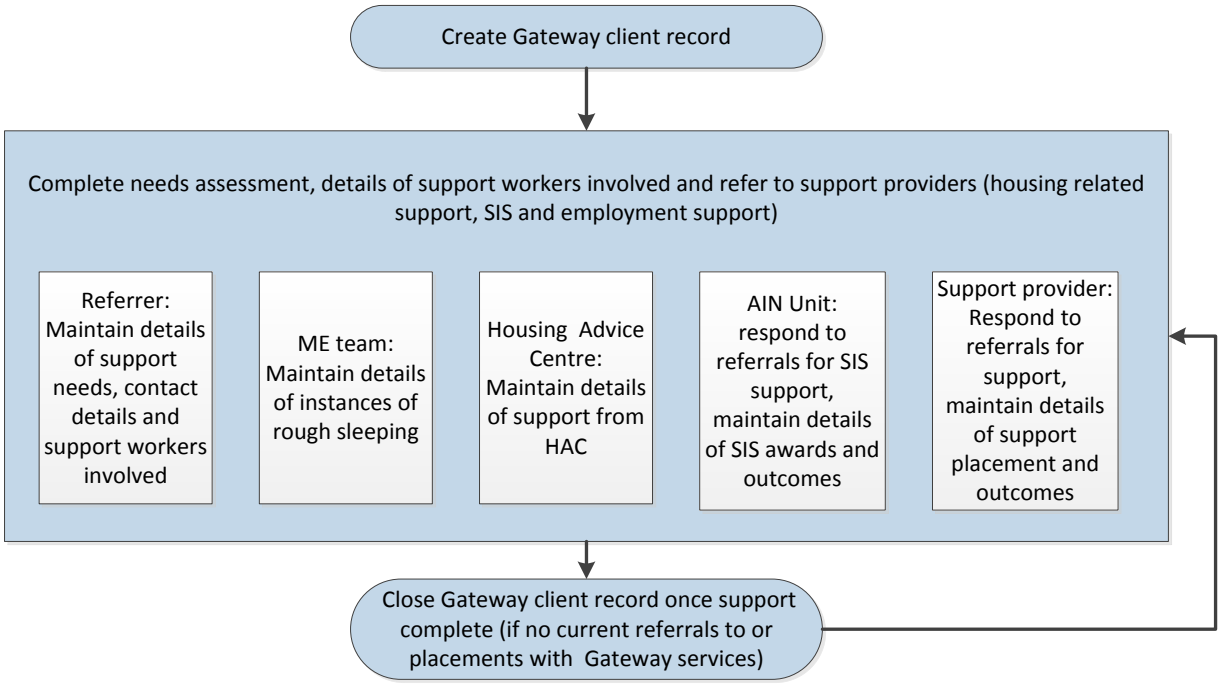
communicated to all other signatory agencies and any necessary action to amend the agreement will be taken.

Clients may make Subject Access Requests (SARs) to any agency which holds data on them. Any agency which receives a SAR in relation a client on the Gateway may discuss this with Newcastle City Council who will be able to offer guidance on releasing their Gateway information.

3. INFORMATION SHARING PROCEDURES & PROCESSES

3.1 Methods of Requesting and Transferring Information

Client information will be transferred via an online client record which will be completed by the partner agency, who will also identify a specific staff member as the case owner with responsibility for keeping the electronic record up to date with details of needs and required support services. Once the client record has been created and assessment completed, referrals can be made via Newcastle Gateway to the support providers identified as appropriate for the client. Support providers will act upon information shared and update the Gateway with responses to referrals and details of any support placements. If necessary, support providers can also refer their clients to additional support by creating a new assessment and referrals.



When a case owner ceases to support a client, the case owner can be changed to another Gateway user if necessary, and details of any changes to the case owner are automatically saved on the client record. The client's record can also be closed if they are not seeking or receiving any further support from services, and details are automatically saved on the client record. Cases can be reopened and reassigned should the client need support from Gateway services in future.

Additional client information may be requested from referral agents by providers, where this is relevant and necessary to their decision, on an ad hoc basis. These requests may be made via Newcastle Gateway or other mediums. Other partner agencies involved with the client may also become aware that additional relevant information exists; in this instance agencies should alert the client's case owner who can update the client record.

3.2 Frequency of Transfer

Information will be transferred between partners as necessary. As information can be transferred electronically between multiple partners via the Newcastle Gateway, it is likely that information will be exchanged on a daily basis.

3.3 Information Standards

It is essential that information exchanged via the Newcastle Gateway is relevant, comprehensive, accurate and up-to-date. The assessment form prompts partners to enter specific client information and, where a client is identified as having a particular need, posing a specific risk or being involved with another agency, entering further details are mandatory.

Where there is a dispute between partners regarding information quality or accuracy, partners should in the first instance inform the AINU, who will take any necessary actions to remedy the situation and provide feedback to all partners.

Responsibility for information shared lies with each user, with the case owner having overall responsibility for ensuring live records are kept up to date with details of needs and required support, and closed when support is no longer provided or required.

Partner organisations will be Data Controllers for information entered onto the Newcastle Gateway by their employees. Organisations may also be Data Processors if they work on information supplied by other organisations, for example by responding to referrals. Given the diversity of information collected via Gateway, signatory organisations are generally expected to hold both roles.

3.4 Retention of Shared Information

Clients' electronic Gateway records will be closed when support is no longer provided by either a partner agency making referrals, or a support provider. Case owners are responsible for closing their own cases. The AINU will routinely check for cases assigned to closed user profiles and reassign or close these as necessary.

Responsibility for information shared lies with each user, with the case owner having overall responsibility for ensuring live records are kept up to date with details of needs and required support, and closed when support is no longer provided or required. Newcastle City Council will be responsible for the retention, storage and secure destruction of electronic client records on the Newcastle Gateway. This will be achieved in partnership with CDPSoft in accordance with CDPSoft's security arrangements. Should the agreement with CDPSoft come to an end, all data will be

returned to Newcastle City Council who will assume responsibility for its retention, storage and secure destruction.

Partner agencies will be responsible for retention, storage and secure destruction of any hard copy information obtained from the Gateway. Hard copy data should be retained only for the period during which it is in use and should then be destroyed by shredding.

3.5 Security of Shared Information

The Gateway software is provided by CDPSoft and is subject to their security arrangements, including maintenance of an SSL certificate, regular penetration testing by IBM Rational Appscan, as well as additional measures to prevent URL hacking, Crosssite Scripting and SQL Injection attacks in accordance with Open Web Application Security Project (OWASP) guidelines. CDPSoft will ensure via these provisions that the transmission process is free from any unauthorised or unlawful interception or access.

The AINU will be responsible for contingency planning in the case of loss of connectivity to the Gateway, and providing off-line solutions. The AINU will maintain a list of current Gateway users which may be used to identify security breaches.

3.6 Information Processing and Access to the Information

Responsibility for information shared lies with each user. Partner organisations will be Data Controllers for information entered onto the Newcastle Gateway by their employees. Organisations may also be Data Processors if they work on information supplied by other organisations, for example by responding to referrals. Given the diversity of information collected via Gateway, signatory organisations are generally expected to hold both roles.

Each partner agency identifies staff members that require access to the Gateway; each staff member is given an individual user profile for the Gateway which enables individual activity to be monitored and relevant restrictions configured. Information added to Gateway is time and date-stamped, with details of the inputting Gateway user. Any user profile not accessed for three months will be closed by the AINU; this can be reopened later if necessary. Users should never share their profile details with a third party, and any reports of such activity will be treated as breaches of this agreement to be investigated and, if deemed necessary by Newcastle City Council, access withdrawn from the individual/s or agency involved. Partner organisations and their representatives are required to abide by this agreement and the principles of the Data Protection Act 1998 when sharing client information, and lead contacts should ensure all their staff members are aware of their responsibilities.

All users are required to abide by this agreement and the principles of the Data Protection Act 1998. Only a client's case owner, staff from the client's current referral and/or support agency, or a member of the AINU will be able to edit their record. If another user accesses their record, this will be visibly logged on the client's record; AINU routinely check unauthorised access to client records and agencies will have access to review or analyse these logs to detect any misuse. Where a client record

requires updating or needs to be closed, only the case owner, staff from the client's current referral and/or support agency or a member of the AINU will be able to amend the client's record or assessment information. Information can be processed by the AINU and representatives from support providers. Support providers will be required to add updates to a client's record with the outcomes of interviews and allocation decisions, as well as admit and placement information where appropriate.

4. MANAGEMENT PROCEDURES & PROCESSES

4.1 Adoption, Dissemination and Implementation

This agreement forms a vital part of the Newcastle Gateway and is signed by representatives of the agencies listed on pages 1-2 of this agreement.

Gateway operators will have access to training and support from members of the AINU. Partner agencies will be involved in ongoing review and amendment of the Gateway through regular working groups which will feed into the review process.

As described in 3.6 above, all users are required to abide by this agreement and the principles of the Data Protection Act 1998. Each signatory agency will take responsibility for their compliance with data protection legislation and this agreement, which will include maintaining effective organisational information security policies and practices; Newcastle City Council will provide guidance on these issues where concerns arise. The Information Commissioner's Office (ICO) Data Sharing Code of Practice and checklists may also provide useful guidance; the ICO also provides guidance on the responsibilities of Data Controllers and Data Processors in relation to Principle 7 of the Data Protection Act:

> *"Personal data shall be processed in accordance with the rights of data subjects under this Act. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

Partners are expected to publicise this agreement to all staff who have access to Newcastle Gateway and to investigate any reports of poor practice or breaches of the agreement by their staff. Partner agencies are responsible for ensuring the information they upload to Newcastle Gateway is accurate and relevant; once information is uploaded to Newcastle Gateway, Newcastle City Council will assume the role of "data processor" with responsibility for maintaining the online system and processing requests for data subjects' access to personal data in compliance with the Data Protection Act. Reported breaches of this agreement will be investigated by Newcastle City Council and, if deemed necessary by Newcastle City Council, access withdrawn from the individual/s or agency involved.

4.2 Information Governance

Responsibility for ensuring compliance with this information sharing agreement within each agency will rest with the lead contacts listed in appendix 1. Any amendments to this agreement will require agreement from all signatories.

Each signatory agency will take responsibility for their compliance with data protection legislation and this agreement; Newcastle City Council will provide guidance on these issues where concerns arise. The Information Commissioner's Office Data Sharing Code of Practice may also provide useful guidance.

Partners are expected to publicise this agreement to all staff who have access to Newcastle Gateway and to investigate any reports of poor practice or breaches of the agreement by their staff. Partner agencies are responsible for ensuring the information they upload to Newcastle Gateway is accurate and relevant; once information is uploaded to Newcastle Gateway, Newcastle City Council will assume the role of "data processor" with responsibility for maintaining the online system and processing requests for data subjects' access to personal data in compliance with the Data Protection Act. Reported breaches of this agreement will be investigated by Newcastle City Council and, if deemed necessary by Newcastle City Council, access withdrawn from the individual/s or agency involved.

4.3 Monitor and Review Process

The Newcastle Gateway will be subject to ongoing monitoring by the AINU and Gateway operators. All partner organisations will be invited to feed into this process via quarterly working groups and ad hoc queries or complaints to the AINU.

Ad hoc queries or complaints about operation of the Gateway should be directed to the AINU at Newcastle City Council. The AINU will liaise with CDPSoft to take any necessary steps to resolve the complaint. The AINU will advise all partner agencies of the results of complaints by partner organisations as soon as possible and in any event within seven calendar days of their resolution.

5. FURTHER DETAILS

5.1 EFFECTIVE DATE

The effective date for this agreement is to be 5th September 2011.

The agreement will be reviewed on an annual basis.

Latest review: June 2017

Version	Date	Summary of amendments
1.0	05/09/2011	N/A
1.2	05/11/2012	Update of contacts and signatory organisations
1.3	24/09/2015	Update of contacts and signatory organisations, additional explanation of services using Gateway
1.4	27/02/2016	Update of contacts and signatory organisations
1.5	01/06/2017	Update of contacts and signatory organisations, additional explanation of services using and support processes monitored via Gateway, details of data security monitoring measures and data protection requirements for partners, addition of partner ICO registration numbers

Appendix 1: Signatories

Information is initially sent to the following authorised roles:

Gateway Referral Agency	Information Commissioner's Office (ICO) registration number	Contact Name	Role	Contact Details
National Probation Service	Z5679958	Carina Carey	Head of Northumbria NPS (North of Tyne)	0191 478 8051 Carina.carey@probation.gsi.gov.uk
Northumbria Community Rehabilitation Company Limited	Z6143637	Louise Mann	Head of Business Change	0345 608 0204 louise.mann@sodexo-justice.scc.gsi.gov.uk
Northumberland Tyne and Wear NHS Foundation Trust	Z691260X	Caroline Wild	Head of Partnerships	0191 223 2994 Caroline.wild@ntw.nhs.uk
Gateway Service Providers	**ICO registration number**	**Name**	**Role**	**Contact Details**
Action Foundation	ZA250308	Richard Hubbard	Director of Operations	0191 2113541 richardhubbard@actionfoundation.org.uk
Changing Lives	Z9183381	Neil Baird	Assistant Director	0191 273 8891 neil.baird@changing-lives.org.uk
Crisis Skylight Newcastle	Z6551446	Andrew Burnip	Director	0191 222 0622 andrew.burnip@crisis.org.uk
Depaul UK	Z6848760	Holly Curran	Newcastle Pathway Manager	0191 209 6705 holly.curran@depauluk.org
Gateshead Housing Company	Z8888060	Catherine Hattam	Housing Options Manager	0191 4332177 Catherinehattam@gatesheadhousing.co.uk
Haven (Tyneside) Limited	Z1361052	Bryan Watson	Manager	0191 477 5605 bryanwatson@haventyneside.co.uk
Home Group Limited	Z7530875	Sarah Anderson	Partnership Manager	0191 260 6100 sarah.anderson@homegroup.org.uk
Karbon Homes Limited	ZA246000	Jennifer Scott	Supported Housing Operations Manager	0191 223 8307 Jennifer.scott@isoshousing.co.uk
Keyring Living Support	Z5081866	Catriona Hackney-	Supported Living	07917 686 658

Networks		Huck	Manager	catriona.hackney-huck@keyring.org
Mental Health Concern	Z4639161	Scott Vigurs	Director of Services	0191 217 0377 scott.vigurs@mentalhealthconcern.org
Mental Health Matters	Z6769210	Jackie Holme	Locality Manager	01642 283 316 JHolme@mhm.org.uk
Newcastle City Council	Z5827702	Ewen Weir	Director for People	0191 278 7878 ewen.weir@newcastle.gov.uk
Newcastle Futures Limited (registered under Newcastle CVS)	Z6434900	Gillian Hewitson	Chief Executive	0191 230 2970 gillian.hewitson@newcastlefutures.co.uk
North of England Refugee Service	Z6720048	William Leong	Housing Projects Manager	0191 245 7301 wl@refugee.org.uk
Phoenix Futures	Z5753869	John Doohan	Service Manager	0191 273 6839 John.doohan@phoenix-futures.org.uk
Places for People	Z6047844	Kathryn McClafferty	Manager	Kathryn.mcclafferty@placesforpeople.co.uk
Praxis Service	Z7915558	Paula Gillingham	Support Service Manager	0191 273 4558 paula.gillingham@btconnect.com
Richmond Fellowship	Z5557991	Karyn Ainsley	Locality Manager	0191 296 0967 karyn.ainsley@richmondfellowship.org.uk
Shelter	Z6483620	Tracy Guy	Area Manager	0344 515 1601 Tracy_guy@shelter.org.uk
St. Vincent de Paul Society	Z8661631	Sean Mallaburn	Service Manager	0191 261 1187 seanm@svp-tyne.org.uk
The Albert Kennedy Trust	Z2481718	Lucy Bowyer	Supported Housing Manager	0191 281 0099 lucy@akt.org.uk
Thirteen Group	Z4811585	Zoe Holley	Service Delivery Manager	0191 2146645 Zoe.holley@thirteengroup.co.uk
Tyne Housing Association Ltd	Z6531963	Michael Nevin	Director of Housing	0191 2284922 michael.nevin@tynegroup.org.uk
Your Homes Newcastle	Z8851643	Lisa Phillisкirk	Assistant Director for Support Services	0191 2771144 Lisa.Phillisкirk@yhn.org.uk
Gateway Support Partners (SIS)	**ICO registration number**	**Name**	**Role**	**Contact Details**
Action for Children	Z8506252	Caroline Herbert	Children's Services Manager	0191 272 4990 caroline.herbert@actionforchildren.org.uk

Advocacy Centre North	Z6434900	Paul Whitlock	Senior Advocacy Coordinator	0191 235 7013 paul.whitlock@cvsnewcastle.org.uk
Affinity Sutton Homes	Z2867413	Jayne Tweedy	Manager	07769671139 Jayne.tweedy@affinitysutton.com
Barnardo's Pause Newcastle Project	Z5951768	Claudene Cetinoglu	Service Manager	0191 284 1905 claudene.cetinoglu@barnardos.org.uk
Bernicia Homes	Z1224454	Gemma Alderson	Team Leader: Intensive Housing Management	07970098015 Gemma.alderson@bernicia.org.uk
Byker Community Trust	Z3316071	Philip Ambrose	Financial Controller and Company Secretary	0191 2903910 Philip.ambrose@bykerct.co.uk
Change Grow Live (CGL)	Z9124986	Carmel Wade	TBC	0191 261 5610 Carmel.wade@cgl.org.uk
Newcastle Carers Centre	Exempt from registration	Katie Dodd	Chief Executive	0191 275 5060 Katie@newcastlecarers.org.uk
The Guinness Partnership	Z3322105	Peter Hedderly	Executive Director I.T and Business Change	01642 987859 informationmanagement@guinness.org.uk
Two Castles Housing Association	Z5599967	Anna Bates	Lettings and Neighbourhoods Manager	01228 635491 Anna.bates@twocastles.org.uk

Appendix 2: Technical Summary

Frequently Asked Questions on Security and Data

Who is the actual hosting company?

Datacenta Hosting Limited based in Bournemouth, United Kingdom. Datacenta is a leading provider of secure hosting, network connectivity, on-line backup, email and Internet Access Security solutions. The majority of CDPSoft's commercial deployments are on Datacenta servers. Datacenta provide highly-resilient technical solutions to Central Government, Local Government, world-class Member Associations and web application development organisations.

How long have they been in operation?

12 years.

How is legal and regulatory compliance assured?

Through various procedures within the regulatory framework of ISO27001 and ISO9001. All issues and changes associated with Policies and Standards are discussed on a standard agenda at Datacenta Monthly Management meetings.

Where will our data be geographically located?

In Bournemouth (United Kingdom) in a concrete and steel subterranean hosting facility utilising steel-protected connectivity routes. The secure back up facility is in Clayford, 20 minutes (8 miles) away from the main facility. No data leaves the UK at any point in time.

How securely is data handled?

- Data is held on servers that are protected by twin firewalls operating double NAT.
- Data is encrypted using Blowfish algorithm.
- Servers operate Active Server/Host Intrusion software at all times.
- MacAfee appliance traps viruses and host intrusion.
- Netforce is used for external security vulnerability testing.
- All data is transmitted in SHA-256 bit encryption.

How is service availability assured?

Datacenta operate 24x7 manned services and support plus have a wide range of automated server management tools for both connectivity and server intrusion. Application availability is managed using Nagios.

How is identity and access managed?

Only authorised Datacenta staff may enter the main or back up facility unless escorted under approved Visitor procedures. Datacenta utilise dual perimeter locks, electronic key fobs, WebAccess CCTV and RedCare Alarm systems. Interior/secure areas require dual key access.

How would our data be protected against privileged user abuse?

Access to the application can be restricted by IP Range and by Time to ensure that access is only available in certain locations and at certain times. Rolling audit logs are also in permanent operation with forensic audit capability. CDPSoft would be happy to discuss other methods of protection.

How often would our data be backed up?

Datacenta operate main server backups on a continuous automatic repeating cycle with offsite backups taken to a secure secondary location and 'firesafed' on a weekly basis. Database/applications are backed up daily as a minimum (more often in the event of application upgrades/patches).

What levels of isolation are supported?

CDPSoft operates separate database schemas for clients of shared server within a common database instance with separate folder structures. CDPSoft operates 5-10 live customers per main Datacenta server.

How are the systems protected against internet threats?

Through the use of HTTPS secure web addresses (SHA-256 encryption) and through the use of a variety of server/host intrusion processes that operate behind twin firewalls operating double NAT. MacAfee appliance traps viruses and host intrusion. Netforce is used for external security vulnerability testing. Application access is via unique user name and password combinations.

How are activities monitored and logged?

Application activity is logged in the Oracle database in a rolling log file which has a full forensic audit capability. All audit data can be extracted from the database using standard SQL queries (e.g. recording the changing of data by a using before and after every click of a Save

button). The more common audit points (e.g. client status changes etc.) are always visible in the respective 'Events' logs.

What certification does the hosting service have?

- ISO27001 equivalent.
- ISO9001 Quality Management.
- ISO 14001 Environmental Management standards.

If / when a contract period expires, how portable is our data (allow for migration from one provider to another, or back in house)?

CDPSoft would produce a database extract in Oracle with a full data dictionary. The extract would need to be signed for and collected in person by an authorised representative. This would be charged as a two day exercise.

Do you carry out Vulnerability Assessments or Penetration Testing?

Both. Every year, CDPSoft completes two processes that are independent of each other:

1. **Vulnerability Scan and Assessment** by a Partner using the latest automated tools such as IBM Appscan.
2. **Full Penetration Test** by a 3rd Party Security Consultancy using a combination of the latest manual ethical hacking techniques and automated tools.

Findings from these exercises are assessed for genuine issues and any corrective actions undertaken as a development priority and documented as part of a re-test.

B) Technical Information

B1) Platform Application Architecture – Technologies

The SHARP product is a web based application accessed by users via their Web Browser. It is currently built using the following core software development 'stack':

Technology	Purpose
Java 7	Programming Language.
Spring 1.2	Open source web application framework.
Apache Struts 1.2	Open source web application framework for developing Java EE web applications using Model View Controller (MVC) pattern.
Apache Tomcat 7	Open source web server and servlet container.
Hibernate 3.2	Hibernate is an open-source object-relational mapping (ORM) library for the Java language which provides a mapping from Java classes to database tables.
Jasper Reports 5.6	Open-source source Java reporting tool.
iText 2.1	Open source library for creating and manipulating PDF files in Java.
Spring Web Services 1.2	Open-source web services framework.
Mule ESB Hub V2.2.1	This is an additional Open-source component that is used, where required, to access web services provided by third party applications such as an interface to a Gazetteer service. It is not required to link to the St Andrew's Supporting People web service.
Oracle 11g	Database.

B2) Performance

SHARP provides an optimally designed hosted environment underpinned by:

- An Apache Tomcat Application Server running on a virtual machine in a private cloud. Extra memory and disk space can be allocated very quickly as the application usage increases.
- An Oracle 11g database which is continuously monitored for performance by an external Database Administration partner.

B3) Resilience

SHARP provides a hosted solution which they have stated is designed to deliver 98.8% availability. The hosted service is provided from an ISO27001 Information Security and ISO9001 Quality Management Tier III data centre. Environment conditioning is currently provided by three 40% utilised refrigerated air conditioning units. Their hosted solution has the following key features to deliver resilience:

- ISO27001
- ISO9001
- Working towards ITIL accreditation and ISO14001
- Business continuity, dual hosting sites in the event of denial of access to the primary location
- Humidity, smoke and moisture monitoring linked to email / SMS notification direct to the operator's team.
- Warm standby policy offering 4 hour recovery as standard.
- Software patched to current release. Patching and updates will be maintained for the life on the installation.
- Host Intrusion Prevention application is to be installed in addition to Perimeter; IS27001 and dedicated Firewall installations.
- Host Intrusion Prevention (Host IPS) for Servers, monitors and blocks unwanted and suspect activity and threats. Host IPS for Servers maintains server uptime and protects assets like applications and databases. It utilises multiple methodologies, including signature and behavioural intrusion prevention, a system firewall, and application-blocking controls with automatic vulnerability shields and security content. Host IPS will be updated and maintained for the life of the installation.
- All systems sit behind firewalls and packet-shaping technology to ensure reliability of service (and not merely connectivity).
- Data is transmitted in SSL mode (HTTPS) with a minimum of 256 bit encryption.
- Backups are daily to HDD online storage server.
- Daily images are retained for up to 90 days.

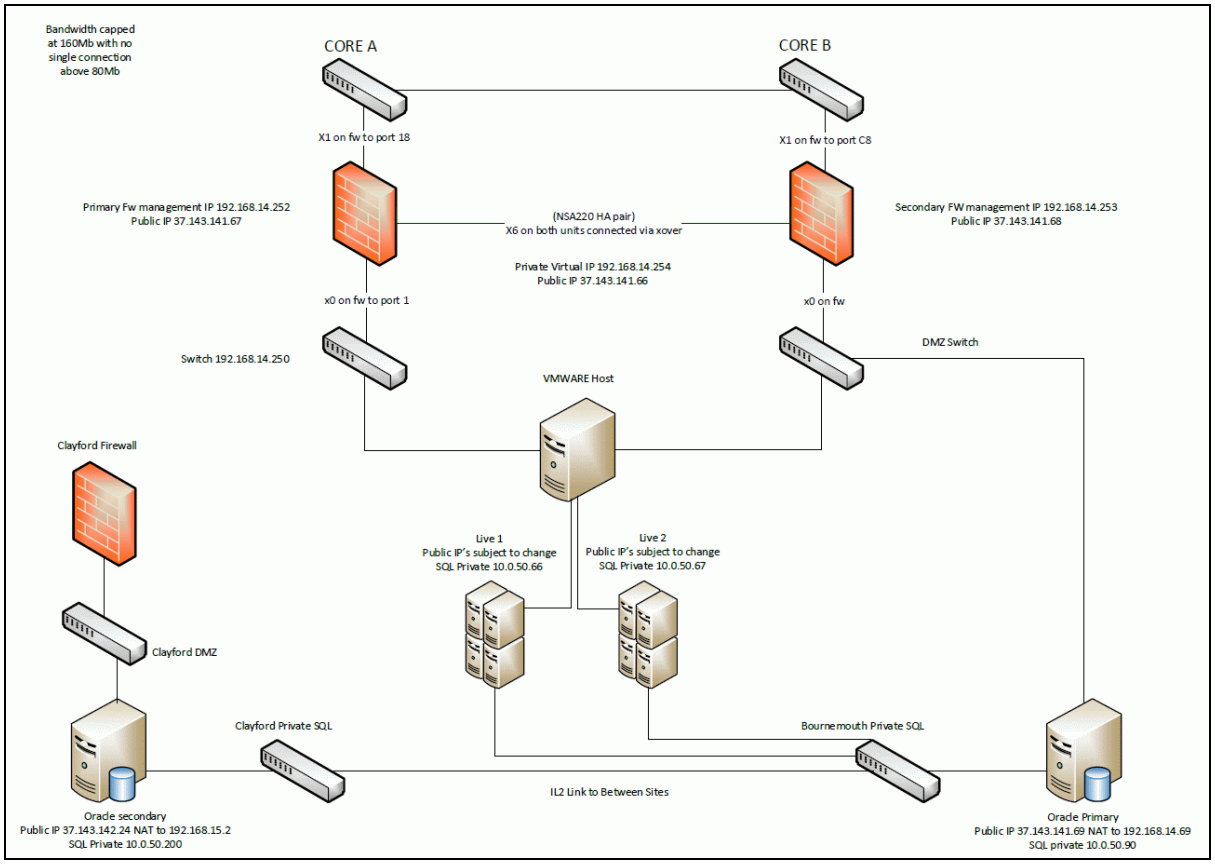
- All backups are held on a secure device, accessible from only the data centre network.
- Datacenta also have mirrored facilities for secure off-site backups and resilience.
- The data integrity of the backup is tested using automated tools over night to ensure they can be restored. Two independent backups are maintained.

B4) Security

- The SHARP primary data centre is provided by Datacenta and is located in Bournemouth. The key security features include
- The primary environment is located in a sub-terrain, steel-reinforced concrete shell.
- There are externally monitored alarms.
- The site is fully protected by CCTV.
- Access control is by access fob, physical key controls and CCTV.
- A one hour UPS protection system is in place and a dual power capability for mains grid electricity supply and cold standby generators.
- SSL encryption to transmit documents and data safely and securely over the Internet.
- AVG Security is in operation.
- All servers operate with twin firewalls operating double NAT between them and with active server/ host intrusion software operating at all times.
- Access to Tier 1 IP is provided by steel-protected, diverse-routed, fault-tolerant circuits.
- The hosted service offers CLAS-accredited and security-cleared personnel, to the highest levels attainable.

B5) Logical Infrastructure Architecture

High Level SHARP Hosting Diagram



The diagram above is a representation (in that the number of Virtual Servers will be greater than two) of the architecture of the hosting environment.

Key points are:

- Dual internet connections, firewalls and switches for resilience.
- VMWare hosted virtual servers for application server resilience and easier capacity management.
- Physical Oracle database server.
- Secondary location database server with near up to date database copy.

B6) Disaster Recovery

SHARP offer a Disaster Recovery environment hosted on and off-premises. Continuous rotating weekly and daily backups are taken. Daily backups are maintained on site where as weekly backups are held off site. Where more frequent backups are required, journals can be secured and transported via secure dedicated network connection to our Disaster Recovery site within five minutes of the data being produced.

Continuous backups can be provided to a resolution down as far as 15 minutes. Protected or restricted data can be encrypted at source and stored at out Disaster Recovery site using 448 bit key cipher.

Data is stored at our Disaster Recovery site which is 15 minutes away from our Primary site and is available for use during disaster recovery. The data integrity of the backup is tested using automated tools over night to ensure they can be restored. Two independent backups are maintained.

We have recently introduced an increased level of database resilience with a near up to date copy of the Oracle database hosted at the secondary geographic location. The database logs from the primary database are copied to the secondary location at frequent intervals during the day and are applied to the database copy. After a failure of the primary database we would switch all application servers to use the secondary database with only the loss of very recently entered data. The recovery time to normal operation would be much reduced compared to data recovery from database backups.

Logical Environments

There will be a single Production environment hosted by our hosting partner.

SHARP will be hosted on shared infrastructure. The Tomcat application servers are hosted on Virtual Machines in a private cloud.

The Oracle database is hosted in a physical server.

Shared infrastructure will be utilised to host each customer SHARP system. Each customer has a dedicated Tomcat application server on a shared virtual server and a dedicated database schema within a shared database server.

The Web Front end will be Internet facing and will be hosted in a firewalled Internet DMZ, the Database Backend will be hosted behind a secondary firewall.

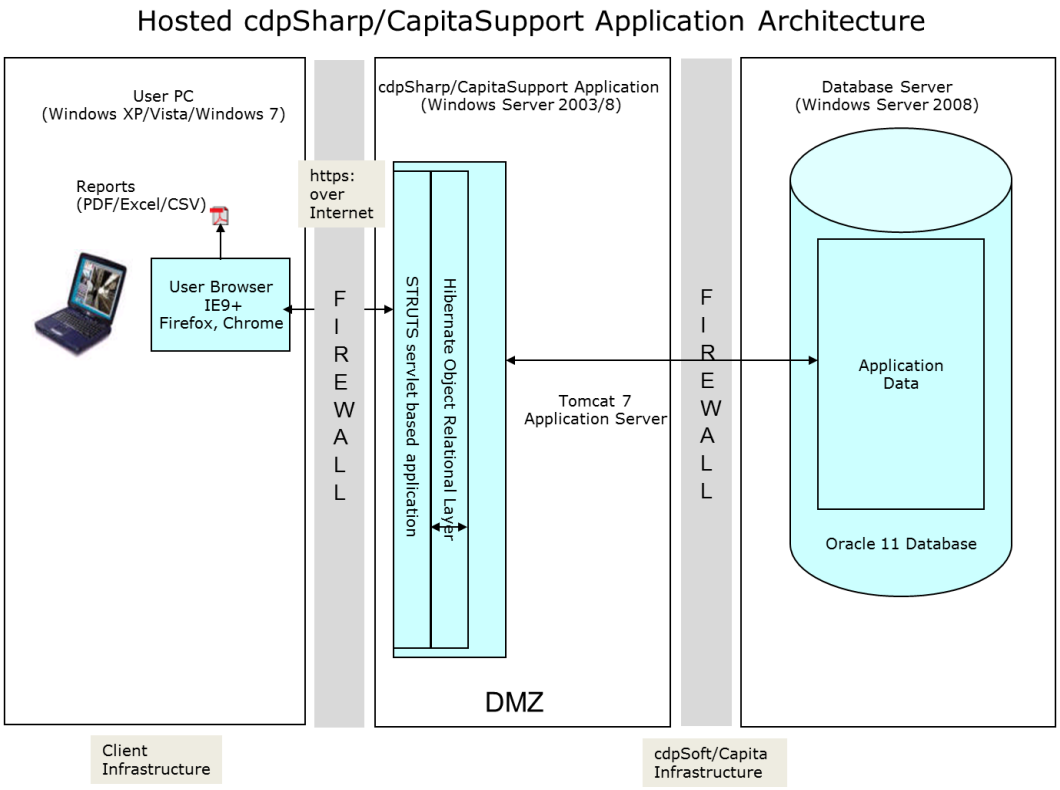
B7) User PC Browser

The user PC can be any standard desktop pc or laptop with the following specification:

Component	Minimum	Recommended
Processor (CPU)	2.33 GHz Intel Core Duo or Above	2.33 GHz Intel Core Duo or Above
Memory (RAM)	2 GB	2GB
Display	1024 x 768 resolution or above	1024 x 768 resolution or above
Free Disk Space	250MB (useful for storage of downloaded files and reports)	500MB
Network (TCP/IP)	10/100Mbps LAN Card	10/100/1000 Mbps LAN Card
Browser	Internet Explorer 9 or above	Internet Explorer 11 or above

	Chrome V30 or above Firefox 10 or above	Chrome V35 or above Firefox 10 or above

B8) Architecture Components



The architecture diagram shows that the SHARP Platform consists of three distinct parts:

1. The Oracle Database Server which stores the data used by the application.

2. The Tomcat Application Server which hosts the application itself.

3. The user PC Browser that is used to interact with the application.

Scalability

The Tomcat application servers are hosted on VMWare managed Virtual Servers. Memory and Disk space can be allocated dynamically to match the resources required as customer usage of the product increases.

The Oracle database server is subjected to continuous capacity planning to ensure that memory and disk space are available to be added at short notice as database use increases.

B9) Interfaces

Internal Interfaces

The following programs are required in order for

- Web Browser.

  The SHARP offering supports the following Web Browsers:

  - Internet Explorer 9, 10 & 11
  - Google Chrome
  - Firefox

- Outlook.

  - Using the 'Tasking' feature SHARP has a facility that can populate an Outlook calendar entry for the logged on user.

- Microsoft Excel for Reporting.

  - Using the built in reporting feature, reports can be generated in excel (.xls) format.

- Microsoft Word for Generating Letters / Reporting.

  - Using the built in reporting feature, letters or reports can be generated in Word.

- Adobe Reader.

  - Using the built in reporting feature, reports can be generated in Adobe.

B10) Communication Protocols

The web application will be available to customer users using an SSL connection using the standard port 443.

B11) Information Security and Governance

Authentication

Access to SHARP is via a URL specified by SCC. The URL uses an SLL connection start (https) creating a secure connection between client and server.

Access to SHARP is via a username and password system. CDPSoft recommends the using individual usernames per system user.

User classes can be sub-allocated by team, provider or service also through the normal use of SHARP.

CDPSoft can enforce a specific format and change interval for Passwords (e.g., eight letters with at least one alpha, numeric, lower and upper case changed at three monthly intervals).

Security Principles

The service will be housed in a partner (Datacenta) data centre, located in Bournemouth, the key physical security principles include:

- ISO9001
- ISO27001 standard for security management
- Working towards ITIL accreditation and ISO14001
- Server rooms are a restricted access zone that is protected with dual security locks and only appointed personnel approved by the Hosting Facilities Manager have access.
- All systems sit behind firewalls and packet-shaping technology to ensure reliability of service (and not merely connectivity).
- Access Tier 1 IP is provided by steel-protected, diverse-routed, fault-tolerant circuits.
- The hosted service offers CLAS-accredited and security-cleared personnel, to the highest levels attainable.
- Tightly controlled entry, with strict procedures in place to monitor and control visitor access both into and within the data centre.
- SSL encryption to transmit documents and data safely and securely over the internet.
- Password policies that control and protect from unwanted access.

B12) Management Services

Backup

CDPSoft offer a Disaster Recovery environment hosted on and off-premises. Continuous rotating weekly and daily backups are taken. Daily backups are maintained on site where as weekly backups are held off site.

- Backups are daily to HDD online storage server.
- Daily images are retained for up to 90 days.
- All backups are held on a secure device, accessible from only the data centre network.
- The Oracle database is mirrored to a standby server at the secondary geographic location. Primary database logs are transferred at regular intervals and are applied to the standby database. If the primary database were to fail the first level of recovery would be to switch to the secondary

database, which would be only 'minutes' behind the primary database in terms of data content.

Summary of items 'back up' items not included in the agreed contract:

- Backup by request is not included within this service but can be provided at an extra cost.
- Recovery by request is not included within this service but can be provided at an extra cost.

Monitoring

Our hosting partner provides 24x7 monitoring of all aspects of the hosted infrastructure from firewalls to the servers themselves.

Our Oracle DBA partner provides expert Oracle database monitoring with dedicated monitoring scripts that run 24x7 at regular intervals.

We directly monitor all aspects of application performance and availability. The Nagios monitoring tool is used to check application availability on a 24x7 basis and all errors generated during customer usage are automatically emailed directly to our support desk.

Antivirus

Antivirus protection is provided at hardware firewall level by our hosting partner.

Patch Management

Our server operating system is either Windows Server 2008 or 2012. We work with our hosting partner to ensure that all urgent and non-urgent Windows patches are installed in accordance with Microsoft recommendations.

We work with our Oracle DBA partner to ensure that the Oracle database is patched in accordance with Oracle recommendations.

There are two production version of SHARP at any time, except of course during a rollout period for a new version. All customers have the same Mainstream Live version of the software with local configuration controlled by property settings. New releases are designated as the Lead Live version which customers are migrated onto. When all customers have been migrated to the Lead Live version, it is re-designated as the Mainstream Live.

We release patch updates to all customers using our automated patch delivery system. Each patch generally contains a 'rolled up' set of fixes.

Non-urgent patches are usually applied outside working hours with no system downtime required, apart from when a server reboot is mandated.

Security Monitoring

Our hosted infrastructure is protected by hardware firewalls with full Antivirus protection.

Denial of Service (Dos) monitoring runs continuously and measures are taken automatically to deal with the threat (e.g. blocking of IP addresses) according to industry best practice.

External access is locked down to port 80/443 only. All port 80 requests are forced to SSL on port 443. The only other open ports are port 22 for inbound SSH and port 3389 for Remote Desktop access but both of these are locked down to specific remote IP addresses only.

A 24/7 alerting system is in place to notify our hosted infrastructure partner of security threats. They will then notify and liaise with us as necessary.