



## NHS Partner Portal

Service Description and  
On-boarding Document

Author(s):	Heath Groves MCM, Chris Webb MCM	
Reviewer(s):	Steve Dixon	
Customer:	NHS (Various)	
Version:	1.2	
Doc ID:	SUNDOWN-741682560-10	
Date:	18 April 2017	
Contacts:	Web:	<a href="http://www.sundownsolutions.co.uk/">http://www.sundownsolutions.co.uk/</a>
	Email:	<a href="mailto:Heath.Groves@SundownSolutions.co.uk">Heath.Groves@SundownSolutions.co.uk</a>
	Phone:	02087 980525



1	Table of Contents	
1	Introduction	2
1.1	Background	2
1.2	Audience	2
1.3	Terminology	2
2	System Overview	3
2.1	Internet facing interaction	3
2.2	Data synchronisation with internal source	4
2.3	Encryption overview	5
3	Support	6
3.1.1	System up-time	6
3.1.2	Service Level Agreement	6
3.1.3	System issues	7
3.1.4	Backup and restore policy	9
3.2	Log Retention Periods	10
3.3	Information Request (Log Parsing)	10
3.4	Physical Access	10
3.4.1	Customer Access	11
3.4.2	Sundown Internal Staff	11
3.4.3	Account management	12
3.4.4	Limitations	13
4	Customer Specific Details	14
4.1	URLs	14
4.2	Admin accounts	14
4.3	Renewal date	14
5	NHSPP Specific Terms and Conditions	15
5.1	Acceptable use policy	15
5.1.1	User accounts	15
5.1.2	Storage capacity	15
5.1.3	Annual renewal	15
6	ANNEX A – About Sundown Solutions (Business Rigour)	16
6.1	Company Details	16
6.2	Key Personal	17
6.2.1	Heath Groves, MCM, Managing Director	17
6.2.2	Chris Webb, MCM, Director of US operations	17
6.2.3	Steve Dixon, Chief Technology Officer	17
6.3	Customer Testimonials & References	18

## 1 Introduction

### 1.1 Background

***“If I had asked people what they wanted, they would have said faster horses.”***

*Henry Ford*

The NHS Partner Portal is a proprietary product created by Sundown Solutions to help its NHS clients overcome the common issue of interacting securely with external contacts whilst maintaining overall control of the data, process, workflow, and security of the data exchange.

The current process at present for most NHS clients involves emailing documents backwards and forwards to suppliers. This type of exchange can lead to the following issues:

- Loss of auditing
- Loss of control
- Multiple versions of the truth
- Loss of workflow
- Data sovereignty issues
- Inability to interact with partners in real time

The NHSP solution provides an internet facing double-encrypted HTTPS, secure logon only solution.

This allows you to issue user accounts to external users and upload (or synchronize) content to the portal. You and your external clients can then interact with that content over a standard internet connection from any device.

This way you can keep track of all interactions and implement real time solutions as well as workflows that include external parties, whilst ensuring the interactions are secure.

Please note that this solution – although highly secure – is not designed to be used for sensitive information such as Patient Identifiable Data (PID).

It is to be used for unrestricted content interactions with external parties only.

### 1.2 Audience

This document has been created for any customer sponsor that has signed up for Sundown Solutions' NHS Partner Portal product.

### 1.3 Terminology

The following terminology is used throughout this document

**NHSP** – NHS Partner Portal – The name given to this product

**SE** – Sundown Encryption – The name given to Sundown Solutions patent encryption standard

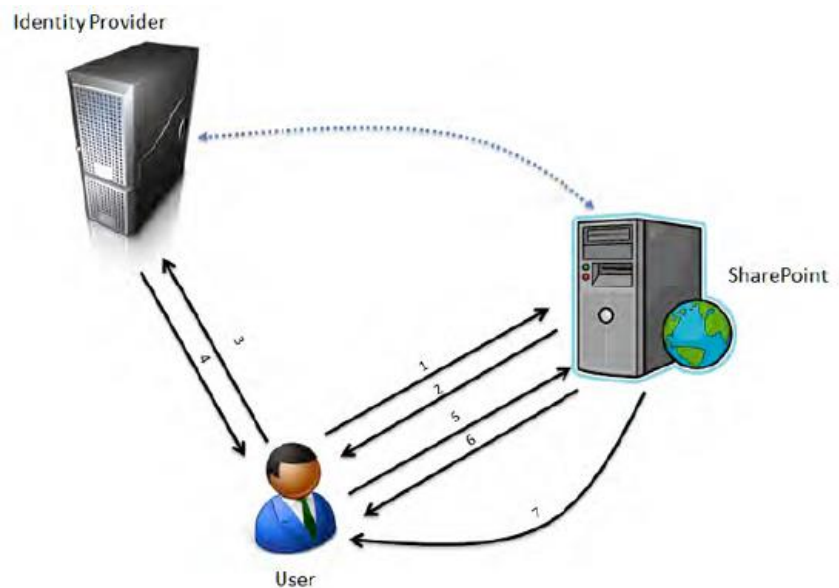
**SSL** – Secure Sockets Layer – A protocol used for transmitting documents securely over the internet

**HTTPS** – Hypertext Transfer Protocol over SSL – the protocol that is used to transfer data between websites securely.

## 2 System Overview

### 2.1 Internet facing interaction

The system itself uses SharePoint Forms Based Authentication in conjunction with wildcard SSL certificates for internet facing exchange



When a new provider requires an account the NHS customer sends the details to [support@sundownsolutions.co.uk](mailto:support@sundownsolutions.co.uk) – The account is created as per the request and the details are sent to the external partner and the customer sponsor.

The account is created in the NHSPP internal domain, which is not linked to any other system and is isolated – it is merely a placeholder for the accounts used in this solution (essentially just a row in an encrypted SQL table).

From this point forward the external provider can use the system as required.

The customer accesses the solution using the accounts granted during the on-boarding process.

## 2.2 Data synchronisation with internal source

In certain circumstances, there is a need to transfer data from an internal source to the external space – it is this transfer of data that is most vulnerable to interception.

These types of exchange are completed using HTTPS and Sundown Encryption.

Sundown Encryption (Patent GB2522096) is a secondary encryption that encrypts all data INSIDE the HTTPS tunnel, essentially ensuring that the data is encrypted inside the encryption – leading to extremely secure data exchange.

The process starts by requesting a synchronized library via support. Once the library is created, you can select the document for transfer and the solution will move the content securely to the NHSP resting place.

## 2.3 Encryption overview

The NHSPP solution (although not for use with restricted data) has been created from the ground up with security as its primary focus. The main way we achieve this is via encryption.

We have created our own encryption patent known as Sundown Encryption (patent GB2522096).

Our encryption works INSIDE normal SSL encryption.

As well as our patented technology, our online portals are protected by GEOTRUST 256 Bit Encrypted Wildcard certificates and only FBA authenticated traffic can hit the portals – http traffic is denied.

The solution encrypts the access to the site in the same way all other internet providers do - using high end SSL certs; when data is transferred from your internal location to the partner portal Sundown Encryption is used INSIDE the SSL Tunnel.

This ensures that all data in-flight is encrypted inside the SSL encryption essentially providing in-flight secondary encryption.

The data in the partner portal is stored on Sundown's enterprise SharePoint farm, this has SQL Encryption enabled as a standard at the DB level and all servers have localised disk encryption enabled at all three of our English sites (Altham, Accrington, and Cornwall). This means the data has absolutely no chance of leaving England, let alone the UK which guarantees data sovereignty.

All Backups are securely encrypted in the same fashion and all drives that store data are also encrypted at rest

Although we do state that our solution is not for PID purposes and is not certified as such, we take our security and encryption very, very seriously – which is why we wrote our own encryption architecture to work inside the standard HTTPS transmission tunnel and then had this ratified by the patent system which was ultimately granted (which is no easy task), as of September 2015.

In short, we encrypt ALL data in flight and at rest – this includes the encryption of all transmission to or from the servers.

## 3 Support

The NHSPP solution has been built from the ground up with security at the core.

The best systems in the world can only be as good as the human interaction that surrounds them. In recent years, the amount of human interaction has been marginalised so hosting companies could reduce overheads and increase revenue streams, whilst automating processes. This in some cases can have a negative effect on overall platform security.

At Sundown, we have a very high level of “administrative overview” with our systems. This means that we ratify all processes and procedures using human interactions – this dramatically reduces the success of “bots” and other synthetic attack vectors.

Although this does increase the timeframe of some support interactions, our customers feel that having a physical member of staff to deal with is far more comforting.

Our support and SLA agreements reflect these factors.

We are also backed by our 24/7 Service Desk product that is available here:

<http://www.sundownsolutions.co.uk/en/Service-Desk.aspx>

### 3.1.1 System up-time

NHSPP is a highly secure system and as such requires an unusually large amount of maintenance and process checking. Due to this, the system must undergo rigorous maintenance and backup procedure. Due to these factors the projected monthly up-time for the system as a whole (including weekends and non-core business hours) is 90%.

However we aim to ensure that we achieve 99% uptime during core hours of 09:00 > 17:00 Monday Friday. All maintenance and tasks are completed outside of this window.

### 3.1.2 Service Level Agreement

The key point to understand here is the definition of the word “Response”. When we respond to a support request from that moment on the SharePoint Administrator has to work that issue to resolution or until the next steps of the investigation are defined. Any support case that comes in (where possible) will be worked immediately, but SLA’s are in place to guarantee communication to the customer and also allow our engineers to focus on upcoming tasks.

For severity one tickets, our engineers know that their current tasks have to be completed within the next 4 hours; within that four hour window they will be working SOLELY on the Sev 1 support case until it is completed.

For Emergencies (as defined below) – response is usually immediate.

**Severity 1** – Response within 4 hours

Used for important cases, that require an immediate fix. The definition of a sev 1 can be termed as:

“All users, cannot get to, access or use some of their data”

**Example** – portal intermittent

**Log call via email:** [support@sundownsolutions.co.uk](mailto:support@sundownsolutions.co.uk)

**Severity 2** – Response within 8 hours

Used for standard issues that require investigation:

“Some users, cannot get to, access or use some of their data”

**Example** – user account request, data restore request

**Log call via email:** [support@sundownsolutions.co.uk](mailto:support@sundownsolutions.co.uk)

**Severity 3** – Response within 3 days

These are general requests for information or clarification and can be categorised as:

“Usually a request for information, training, or infrastructure work”

**Example** – request for logs, auditing information request

**Log call via email:** [support@sundownsolutions.co.uk](mailto:support@sundownsolutions.co.uk)

**Emergency** – Response within 15 minutes

This level of support is customer driven – if the customer feels they have an absolute emergency then they can log a call as such. The definition of an emergency is subjective, which is why the customer can dictate it.

**Example** – NHSP.co.uk is down, require an immediate answer to a question or need to disable an account quickly.

**Log call via phone:** 02087 980525

**Log call via email:** [support@sundownsolutions.co.uk](mailto:support@sundownsolutions.co.uk)

### 3.1.3 System issues

A system issue can be defined as an issue where the customer requires assistance regarding the normal operation of the portal. In such a case, all requests should be logged to the service desk via



email. The request will then be triaged and dealt with based on the criteria laid out in the Service Level Agreement section.

*To log a call email: [Support@sundownsolutions.co.uk](mailto:Support@sundownsolutions.co.uk)*

### 3.1.4 Backup and restore policy

The purpose of this section is to outline the Service Level Agreement when dealing with backup and restores for the NHSPP system. This SLA has been created with the following factors in mind:

- The business-critical nature of the documentation stored on the portal
- The requirements and needs of the end user base
- The data retention requirements of the entire organisation
- The operational cost of maintaining the backup architecture
- The ability to fulfil these commitments to our user base

The following is the recovery path if a customer requires a Restore:

**If the restore request is in the last 7 Days - guaranteed point-in-time restore**

This means we will be able to recover the data/document to a specific point in time. For instance we can restore document X as it was at 11:00am on Tuesday morning.

**If the restore request is over 7 Days, but within the last 14 days - guaranteed daily restore only**

This means that we will be able to restore the data/document to the nearest full (+Differential) daily backup (taken at 20:00 daily). For instance if you require document X from the 21st, the closest we could get is the document as it was at 20:00 on the 20th

**If the request is over 14 days - request will be denied (unless approved from executive level)**

This means we will no longer restore documents past the 14 day point. However, we do take and keep a monthly backup for one month prior. In the very rare fringe cases, if a document is business critical and an executive level member authorises the restore attempt - then we can look into these monthly backups and see if the data/document exists. However, using this mechanism is best endeavour only, and does not guarantee the restoration of data.

In short the overall policy is as follows:

**Within 7 Days - Point-In-Time guaranteed**

**After 7 Days, within 14 Days - Last days backup guaranteed**

**After 14 Days - Request denied (unless authorised at executive level)**

**We only keep backups for a maximum of 28 Days**

To request a restore please log a Sev 2 request by emailing [support@sundownsolutions.co.uk](mailto:support@sundownsolutions.co.uk)

### 3.2 Log Retention Periods

We retain usage logs for a maximum of 7 days – these are the in-depth actions logs inside the system.

We retain Firewall access logs for 28 days.

We retain Access Logs to the system for 12 months.

### 3.3 Information Request (Log Parsing)

From time to time customers may require information requests from the logs. Examples of this could include (but are not exclusive to):

- Reviewing access to a specific document
- Reviewing access to a specific site
- Reviewing permissions of specific accounts

Whilst we give the ability to setup audit and control on the front end of the site collection to the customer we recognise that there can be some situations where an in-depth analysis will need to be performed.

In these cases, the customer raises an email support request to:

[Support@sundownsolutions.co.uk](mailto:Support@sundownsolutions.co.uk)

**Subject:** Info Request: [Customer Name]

**Details:** Details of request

Depending on the nature of the request, will aim to deal with it and return a response inside 28 days. The more specific the request is, the faster the response will be.

We not field requests that are disproportionate to the length of time required to retrieve the information based on necessity – this is a reserved right of Sundown Solutions.

### 3.4 Physical Access

Physical Access to and from the servers is strictly controlled. There are two elements to the physical access component of our system, the customers level of access and Sundown's Internal Staff access, both covered in this section.

### 3.4.1 Customer Access

Customer access is strictly forbidden, except for the customer sponsor (or their pre-approved representative). This type of access is on pre-approval via email from Sundown Solutions and a minimum of 7 days' notice must be given.

If approval is granted, the customer will be under dual escort (2 Sundown Members of Staff) always and will NOT be allowed to logically access the servers i.e. they will not be allowed on a PC, Laptop device or keyboard or mouse whilst on the premises.

If they require their data, then the relevant data will be transferred to them via an electronic mechanism of their choosing, or the physical hard drive of their choice. Sundown staff will be responsible for retrieving this data and placing it into the hands of the customer if a physical request is required, but this will be completed on-site. The customer will then be responsible for removing the data from our location.

All visits to Sundown's offices are logged and tracked via Outdoor and indoor CCTV (audio and visual), IR Motion detectors (internal and external) and internal movement sensors.

### 3.4.2 Sundown Internal Staff

Access to Sundown's server room is by approval only.

In some cases, staff, may need to perform routine maintenance.

The access codes to the server room are changed every 24 hours, and only directors are given this code.

When access is required a request is sent via email to the engineer's line manager who requests authority at the allotted time and date from a director.

If the request is allowed the code is given to the engineer at the specified time, as well as the access request, reason for the request, CAB notes and authorisation request being logged.

Once the reason for the access is complete the access code for the day is reset, and anyone else requiring access must go through the above process.

### 3.4.3 Account management

Account management for the NHSP system is critical. Each person that requires access will get their own account and permissions will be set accordingly.

In order to have these accounts created and managed please follow the below procedure.

#### 3.4.3.1 Creation and deletion

To have an account created please email [support@sundownsolutions.co.uk](mailto:support@sundownsolutions.co.uk) using the following template:

**Subject:** NHSP Account Creation <INSERT CCG>

Please create the following account:

**First Name:**

**Last Name:**

**Organisation:**

**Direct Contact Number:**

**Direct Email:**

**NHS Sponsor:** <the NHS person responsible for the request>

**NHS Sponsor email:**

**Expiry date:**

**Access Required:** <List the system, site, library or list the user is to access>

To have an account deleted email [support@sundownsolutions.co.uk](mailto:support@sundownsolutions.co.uk) with the subject of “account deletion” and list the details of the account you would like to be deleted.

#### 3.4.3.2 Password management

Due to the secure nature of the system, all password resets (and all account management) are dealt with in real time by Sundown staff.

In the first instance, please email the request to [support@sundownsolutions.co.uk](mailto:support@sundownsolutions.co.uk) – if the request is immediate or critical then please call us on: **02087 980525**

### 3.4.4 Limitations

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centres, including at your site or between your site and our data centre);
2. That result from the use of services, hardware, or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services;
3. Caused by your use of a Service after we advised you to modify your use of the Service, if you did not modify your use as advised;
4. During or with respect to preview, pre-release, beta or trial versions of a Service, feature or software (as determined by us);
5. That result from your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;
6. That result from your failure to adhere to any required configurations, use supported platforms, follow any policies for acceptable use, or your use of the Service in a manner inconsistent with the features and functionality of the Service (for example, attempts to perform operations that are not supported) or inconsistent with our published guidance;
7. That result from faulty input, instructions, or arguments (for example, requests to access files that do not exist);
8. That result from your attempts to perform operations that exceed prescribed quotas or that resulted from our throttling of suspected abusive behaviour;
9. Due to your use of Service features that are outside of associated Support Windows; or
10. For licenses reserved, but not paid for, at the time of the Incident.

## 4 Customer Specific Details

This section outlines the customer's specific information

### 4.1 URLs

The URL for your portal is:

### 4.2 Admin accounts

The administrative account for your solution is:

Username:

Password:

### 4.3 Renewal date

The yearly renewal date for your solution is:

## 5 NHSP Specific Terms and Conditions

By utilising the NHSP portal you agree to accept all conditions as laid down in our standard terms and conditions – available [here](#) and on request.

### 5.1 Acceptable use policy

Outlined below is the specific information with regards to acceptable usage

#### 5.1.1 User accounts

The management and creation of external accounts is crucial to the system. As part of the standard provisioning process we allow 50 accounts to be created and maintained by each customer.

Customers requiring more than 50 accounts can negotiate terms based on the required usage for the specific requirement.

#### 5.1.2 Storage capacity

As the solution is for external interaction we allow up to 100GB of storage space in the customers database.

Customers requiring more than 100GB can negotiate terms based on the required usage for their specific requirement.

#### 5.1.3 Annual renewal

The annual renewal date is the date stated in section 4.

All fees are due on the annual date of re-newel.

If the customer no longer requires the solution, then a period of 2 months' notice must be given BEFORE the renewal date.

If the customer terminates service, the customers' database will be provided on a suitable external storage device – or uploaded to a location of the customers choosing.



## 6 ANNEX A – About Sundown Solutions (Business Rigour)

### 6.1 Company Details

Sundown Solutions are a Microsoft Gold Partner specialising in Business Productivity Solutions that build on Microsoft SharePoint, Office 365 and associated web technologies. With a host of development capabilities in .Net, iOS, Dynamics CRM and eCommerce, we are a market leading software provider as well as a security focused market leader in web technologies.

Sundown Solutions have worked at the highest levels in the SharePoint and Cloud sphere for the last decade. We have worked with some of the world's best and brightest organisations, including four years for Microsoft directly.

We offer the highest level of technical ability available in the SharePoint and O365 market place with our world-class team that includes Microsoft Certified Masters, Microsoft MVPs and Microsoft Certified Solutions Masters.

Below is the current company profile and information for your records

<b>Company Name</b>	Sundown Solutions Ltd	
<b>Company Address</b>	Moorside House, Altham, Accrington, Lancs BB5 5TZ	
<b>Company Website</b>	<a href="http://www.sundownsolutions.co.uk">http://www.sundownsolutions.co.uk</a>	
<b>Company Number</b>	6988701	
<b>VAT Number</b>	976 9207 67	
<b>Years Trading</b>	10	
<b>Microsoft Gold Partner ID</b>	1819683	
<b>Frameworks</b>	Digital Outcomes and Specialists 2, G-Cloud 9	
<b>Insurance policies</b>	<b>Public and Products Liability:</b>	£2,000,000
	<b>Employers Liability:</b>	£10,000,000
	<b>Professional Indemnity:</b>	£2,000,000
<b>Bank Name</b>	Royal Bank of Scotland	
<b>Branch Address</b>	119 Blackburn Road, Accrington, Lancashire, BB5 0AA	
<b>Payment Method</b>	BACS Preferred, Cheque payments also accepted	
<b>Account Number</b>	Available upon request	
<b>Sort Code</b>	Available upon request	
<b>DUNS Number</b>	Available upon request	
<b>Standard Payment Terms</b>	Available upon request	

## 6.2 Key Personal

Although Sundown solutions have many employees the following people represent the company board and can be approached/contacted at any time.

### 6.2.1 Heath Groves, MCM, Managing Director

Heath has a wealth of expertise in IT and is highly regarded as one of the world's leading Microsoft professionals, working for both Microsoft directly and through his own business, Sundown Solutions.

His qualifications include Microsoft Certified Master: SharePoint (MCM/MCSM) - High end SharePoint 2013 Solutions Architect/Developer and 14 year MCT equally proficient with both front and backend development.

His experience has covered the whole breadth of the SharePoint product stack, from front end consulting, configuration and solution creation through to the highly customized and bespoke development (including deployment, scripting and engineering).

### 6.2.2 Chris Webb, MCM, Director of US operations

Chris is an expert in SharePoint holds the MCM, MCSM SharePoint, & MCT and a Principal SharePoint architect based out of the Dallas Fort Worth area. He has experience of working directly for Microsoft, as well as Lockheed Martin and other US federal contracting firms. For the past 5 years, he has focused on high security environments and integration with external business systems, primarily government and hospital systems.

With exposure to all elements of SharePoint, from systems architecture to troubleshooting to development, Chris is a premier SharePoint resource. He also volunteers to teach and help build computer science programs in high schools across the US.

### 6.2.3 Steve Dixon, Chief Technology Officer

Steve has 30 years' experience in IT, working in some of the world's largest infrastructure projects. These include Microsoft as the key SQL support escalation engineer for Office365 (cloud services) and DWP Windows XP SP2 OS Refresh rebuilding 150,000 workstations remotely with Zero Touch Deployment as the Technical Lead.

He was also Technical Lead on the NHS Hector (Health Emergency Care through Telematics Operational Resources) to put a "Virtual Doctor" in the back of an Ambulance.

He has in depth working knowledge of all SQL components in large scale technical environments (100,000 users+), for both private and public sector clients including a large proportion of FTSE 100 companies.

## 6.3 Customer Testimonials & References

Specific references can be provided upon request for specific projects but we have a collection of customers happy to be contacted directly out of context to provide references for any of our work.

Organisation/Customer	Project/Product	Contact Details
<b>GMCSU (Shared Service)</b>	Various large scale SharePoint migrations	<b>Jon Shone</b> - Data Centre Project Manager <a href="mailto:jon.shone@mercuryitmanagement.co.uk">jon.shone@mercuryitmanagement.co.uk</a> 07850 942536
<b>GMCSU (Shared Service)</b>	24/7 Service Desk	<b>Jon Shone</b> - Data Centre Project Manager <a href="mailto:jon.shone@mercuryitmanagement.co.uk">jon.shone@mercuryitmanagement.co.uk</a> 07850 942536
<b>Trafford CCG</b>	BedStateTracker.co.uk	<b>Martin Bee</b> - IT Manager Trafford CCG <a href="mailto:Martin.Bee@nhs.net">Martin.Bee@nhs.net</a> 07814 982970
<b>Manchester City Council</b>	BedStateTracker.co.uk	<b>Jonathan Gavin</b> - Manchester City Council <a href="mailto:j.gavin@manchester.gov.uk">j.gavin@manchester.gov.uk</a> 07534 386286
<b>Trafford CCG</b>	NHS Partner Portal Product	<b>Martin Bee</b> - IT Manager Trafford CCG <a href="mailto:Martin.Bee@nhs.net">Martin.Bee@nhs.net</a> 07814 982970
<b>HMR CCG</b>	Company Intranet	<b>Paul Chadwick</b> - IT Manager HMR CCG <a href="mailto:Paul.Chadwick5@nhs.net">Paul.Chadwick5@nhs.net</a> 07825906186
<b>HMR CCG</b>	Company Extranet	<b>Paul Chadwick</b> - IT Manager HMR CCG <a href="mailto:Paul.Chadwick5@nhs.net">Paul.Chadwick5@nhs.net</a> 07825906186
<b>Yourhousing Group</b>	Various SharePoint projects including installation and customised app creation	<b>Neil Beckingham</b> - CTO <a href="mailto:Neil.Beckingham@yourhousinggroup.co.uk">Neil.Beckingham@yourhousinggroup.co.uk</a> 07894 799526
<b>College of Policing</b>	Large scale, highly secure EDRMS project	<b>Diane Downey</b> - CTO <a href="mailto:Diane.Downey@College.pnn.police.uk">Diane.Downey@College.pnn.police.uk</a>
<b>South Yorks and Humberside Police</b>	Development Operations and CSOM roll out + training	<b>Lee Steven Barr</b> - Head of Digital Services <a href="mailto:Lee.stevens-barr@southyorks.pnn.police.uk">Lee.stevens-barr@southyorks.pnn.police.uk</a> 07825 723494