Chief Executive
2 Franklin Street
BELFAST
BT2 8DQ

Tel: 028 9536 3863
Email: FOI.BSO@hscni.net

8th August 2024

BY EMAIL
[redacted]

Our Ref: FOI 2255

Dear [redacted]

Your request for information was received on 11th July 2024 and was dealt with under the terms of the Freedom of Information Act 2000. Please be advised that the Business Services Organisation (BSO) has now completed its search for the information you requested in relation to BSO's Procurement & Logistics Services processes.

Please find a response as follows and enclosed:

Have the documents prepped and ready for procurement procedures? The procurement process would have involved both technical content and commercial content. On the commercial side, was there a RFQ, RFI, RFP, ROI, RFO, Tender etc. How was this process managed?

A Pre-Market Engagement process was completed to inform the development of the tender documents. With regards to the technical content, please refer to the Appendix 1 released under FOI2236 and Appendix 6 and 7 as attached.

With regards to the commercial content, please refer to Appendix 8.

The tender process was completed in accordance Public Contracts Regulations 2015 as an Open Procedure.

In preparation of the procurement documents, there would need to have been professional inspection of site parameters and conditions in conjunction with the complex technical standards for populating BOQ's or BOM's set out for equitable response in quality and pricing. This content may have been by a professional consultant or someone other than a supplier who is

qualified in this diverse and complex speciality field. For example, my professional observation of Ulster Hospital parking infrastructure is that it is not fit for immediate deployment of an integrated ANPR solution.
There are many milestones that need to be achieved before implementation of an integrated ANPR solution.
Furthermore, have the relevant SOPs for an ANPR system been defined? What are these, from a supplier perspective and from an operations perspective?

Please refer to Appendix 1 released in FOI2236 and Appendix 6 and 7 as attached, which sets out the requirements in relation to the contract.

Furthermore, the system and operations would need to be compliant to other legislation such as Freedom of Protection and Data Privacy as set out in GDPR.

Please refer to Appendix 1 released in FOI2236 and Appendix 6 and 7 as attached, which sets out GDPR requirements.

As the 2022 legislation is unique and the chosen solution was ANPR, how was this incorporated into the procurement process?

Please refer to Appendix 1 released in FOI2236 and Appendix 6 and 7 as attached.

The total cost of ownership of this solution (capex + opex e.g. 10yr licenses, maintenance costs and operational expenditure etc.) would also need to be evaluated. How was this provision included for such an evaluation by procurement?

Please refer to Appendix 8 and Appendix 9.

Such a massive undertaking would have required comprehensive details of site audits for all affected HSC estates in NI impacted by the 2022 legislation. All this information would then be combined with the strict deadlines (incl legislation) and other commercial conditions.
My question is where is this information, who compiled it and how was this all achieved in 3 months? Was there a contract for each site, or an overarching contract for all sites?

Please refer to Appendix 1 – 5 and Appendix 1 released under FOI2236.
This information was compiled by each Trust.
A single contract has been awarded for all Trusts.

I hope that the information provided assists you. If you are dissatisfied in any way with the handling of your request, you have the right to request a review. You should do this as soon as possible or in any case within two months of the date of issue of this letter, as the BSO, along with all other public authorities are not obliged to accept internal review requests after this period has lapsed.

In the event that you require a review to be undertaken, you can do so by writing to

Information Governance Manager,

2 Franklin Street,
Belfast,
BT2 8DQ

If, following an internal review, carried out by an independent decision-making panel, you remain dissatisfied in any way with the handling of the request, you may make a complaint under Section 50 of the Freedom of Information Act, to the Information Commissioner's Office and ask that they investigate whether the BSO has complied with the terms of the Freedom of Information Act.

You can contact Information Commissioner at:

Website: www.ico.org.uk
Phone: 0303 123 1113
Email: casework@ico.org.uk
Post: Information Commissioner's Office
3rd Floor, 14 Cromac Place
Belfast
BT7 2JB

In most circumstances the Information Commissioner will not investigate a complaint unless an internal review procedure has been carried out. However, the Commissioner has the option to investigate the matter at his discretion.

Yours Sincerely,

Karen Bailey
Chief Executive

Belfast Health and Social Care Trust (BHSCT)

The BHSCT have 3 hospital sites requesting ANPR and are as follows:

Royal Victoria Hospital (RVH)

The RVH site comprises of 12 carparks – 10 staff carparks and 2 for designated for patients/visitors.

Carpark	Staff/Visitors	Spaces	Number of Barriers in situ	Network infrastructure Present	Number of Proposed ANPR Cameras
1	Visitors	945	4	Yes	12 (all new columns)
2	Visitors	93	2	Yes	4 (all new columns)
3	Staff	-	2 (non operational)	Yes	2
4	Staff	62	2	Yes	2
5	Staff	265	2	Yes	4
6	Staff	485	3	Yes	2
7	Staff	62	0	No	2
8	Staff	336	2	No	2
9	Staff	115	2	No	4
10	Staff	24	1	No	2
11	Staff	178	2	No	3
12	Staff	16	1 (Gate)	Yes	2

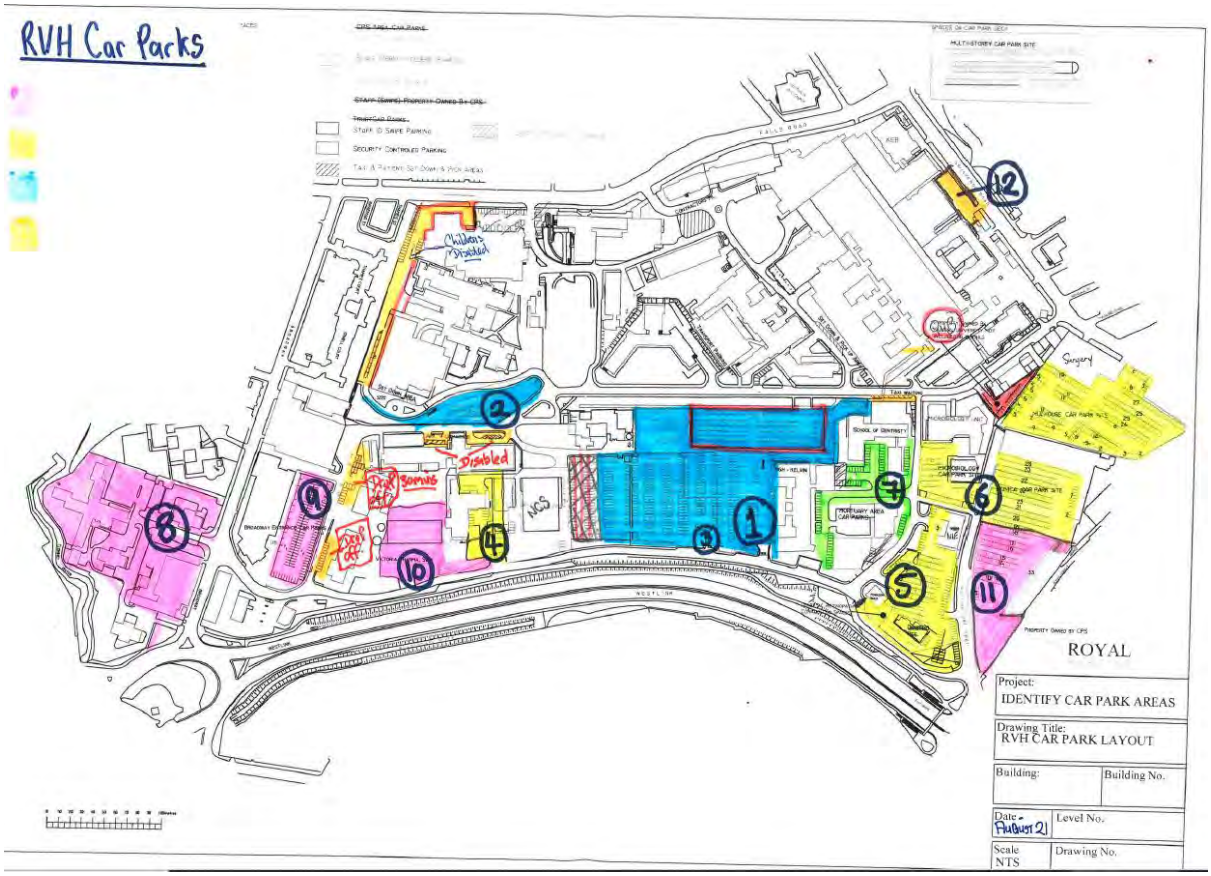
PROPOSED NEEDS

Patient/Visitor Carparks

We would propose Carpark 1 and 2 on map are ANPR operated barriers with a 3 hour parking window for patients and visitors that can be extended via onsite terminals

Staff Carparks

We would propose Carparks 3 to 12 that are staff carparks are operated via ANPR barrier controls and access permitted via a parking permit system.



Belfast City Hospital

The Belfast City site comprises of 11 carparks with a total of 1868 spaces (67 disabled spaces are available on site).

Carpark	Staff	Visitors	Spaces	Number of Barriers in situ	Network Infrastructure Present	Number of proposed ANPR cameras
Donegal Road multi-storey	796	300	1096	6	Yes	12
Tower multi-storey	-	320	320	4	Yes	4
AMHIC	77	30	107	2	Yes	2
Security	-	43	43	2	Yes	2
Radiotherapy	-	51	51	2	Yes	2
DPU	-	35	35	2	Yes	2
Post Grad	40	-	40	2	Yes	2
Estates	30	-	30	1	Yes	1
Transport			88	2	Yes	2
Renal	-	40	40	2		2
Henry Moore			8	2	No	2
Telephony	10	-	10	1	No	1

PROPOSED NEEDS

Patient/Visitors Carparks

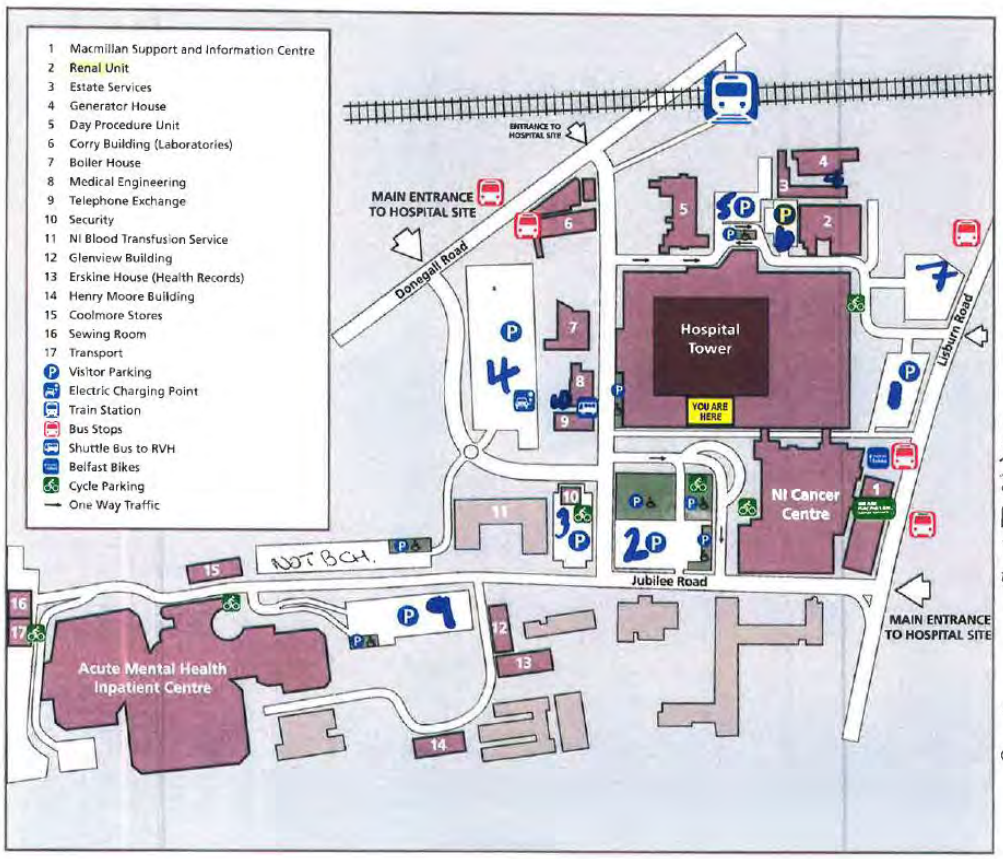
We would propose Carparks with visitor access are APNR operated barriers with a 3 hour parking window for patients and visitors that can be extended via onsite terminals

Staff Carparks

We would propose that carparks that have staff access are operated via ANPR barrier controls and access permitted via a parking permit system.

(note – some BCH carparks need to accommodate both staff/visitors)

* Belfast City Hospital *



1: RADIOTHERAPY
2: TOWER MS
3: SECURITY
4: Donegall Road MULTI
5: D.P.U
6: RENAL
7: POST GRAD
8: ESTATES
9: AMHIC
10: Exchange

Mater Hospital

There are 2 carparks on the Mater site. The main carpark is located at the top of the site and is a mixture of visitors and staff. There are a total of 333 spaces in this carpark. (Estates have a compound that accommodate parking of vehicles.) There are currently 2 networked barriers within this car park (One in and one out). There would be a total of 4 ANPR cameras required for this car park.

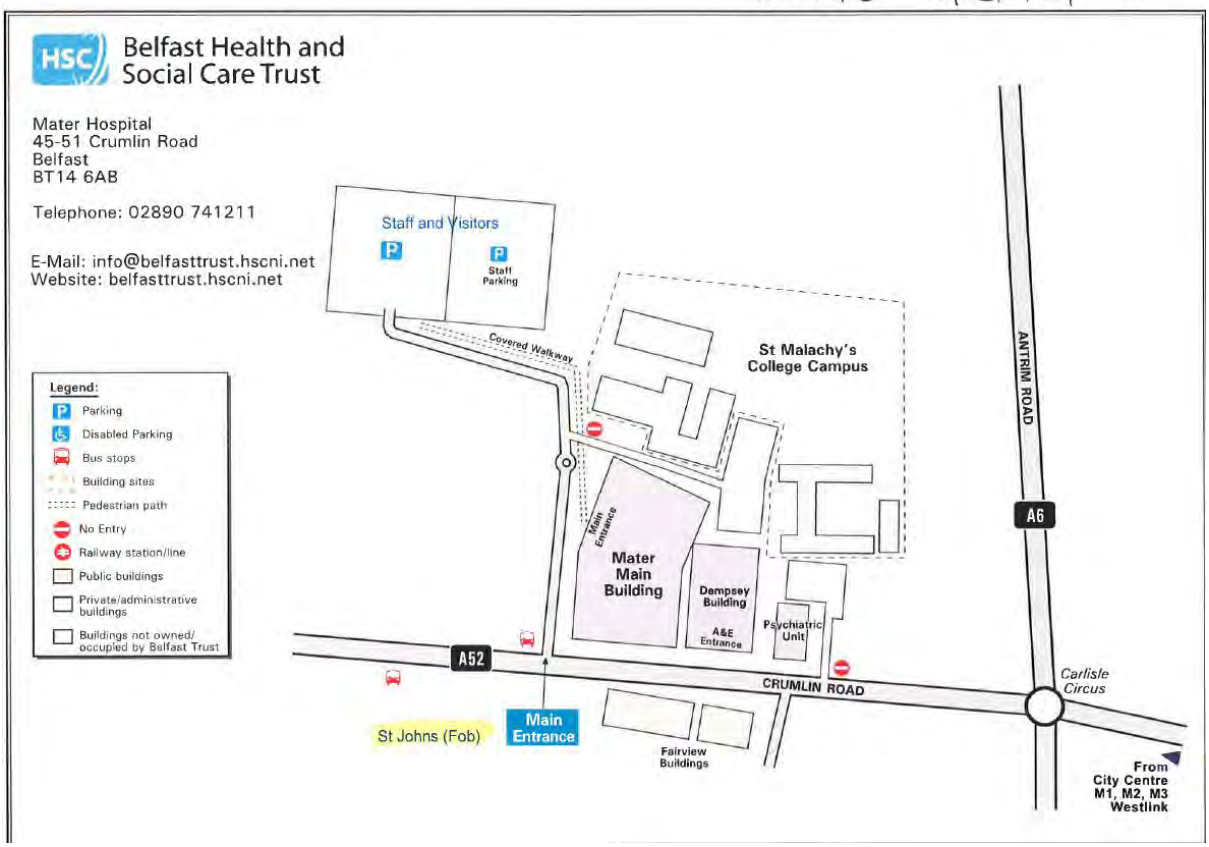
The St John's carpark, accessed via the Crumlin Road, was built to allow for disability access to the main hospital site and to relocate the existing senior medical staff who were previously parking at the front of the Dorrian building. It is accessed via coded handheld-programmed transmitters on an electric gate. There are a total of 52 spaces in this carpark. One ANPR camera would be required in this area

There are 11 spaces at the front of the Mater Hospital, 9 of these are designated for blue badge holders. One ANPR camera required for this area.

It is estimated that a further 6 ANPR cameras would be required in other locations across the site. Actual locations to be agreed on survey.

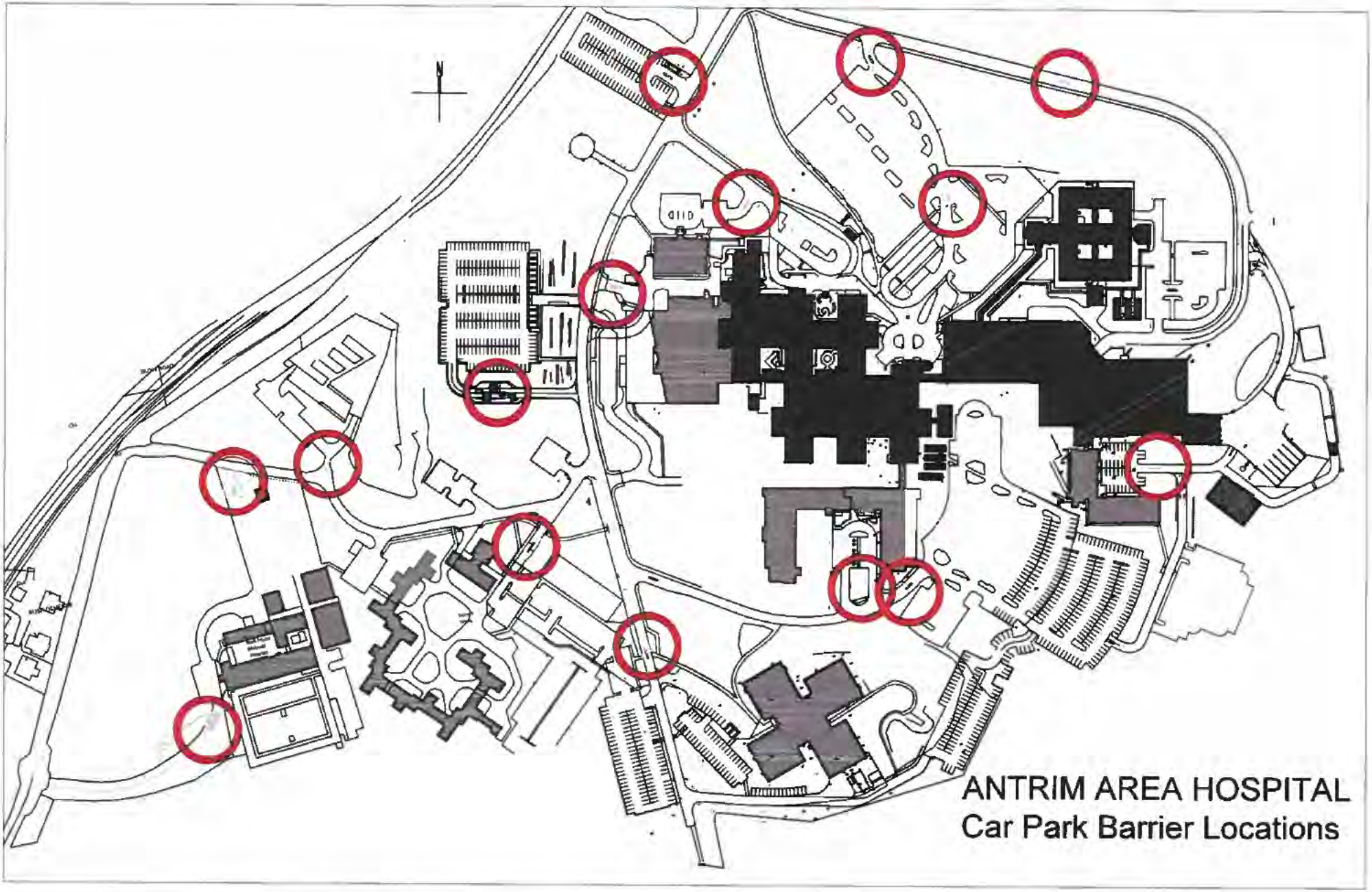
Total Mater spaces: 396

*Mater Hospital *



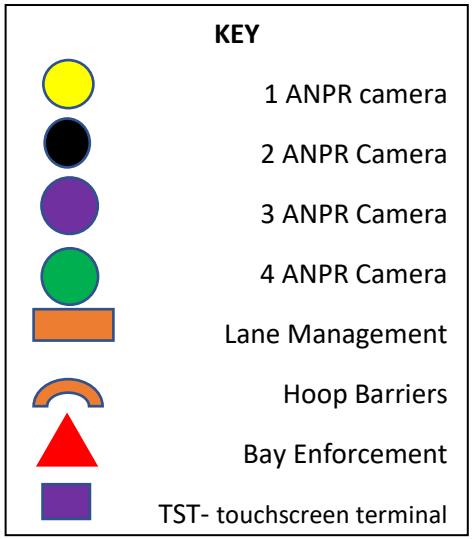
Other BHSCT Requirements for Implementation

- 16 x Self ticketing kits (phone and printer) enabling attendants or other designated Trust staff to enforce 24/7


ANTRIM AREA HOSPITAL
Car Park Barrier Locations


SEE DRAWING 3450/PD/CD2 DETAIL 4
SEE DRAWING 3450/PD/CD2 DETAIL 3
SEE DRAWING 3450/PD/CD2 DETAIL 2
SEE DRAWING 3450/PD/CD2 DETAIL 1
SEE DRAWING 3450/PD/CD4
Refer to Architects drawing for all proposed parking layouts and line markings
Barrier Locations marked in yellow
3450/PD/C01

South Eastern Health and Social Care Trust: Potential ANPR locations



Bangor Hospital:

Main Car Park:

1 ANPR Camera on a new column – hard dig and lane management

Power located: Inside the building

2 terminals inside building

Drop Off Car Park:

1 ANPR Camera on a new column – soft dig

1 ANPR camera wall mounted

Power located: Inside the building

Downe/Downeshire Hospital:

Downshire Hospital:

5 ANPR wall mounted

2 ANPR on a new column – soft digs for all

4 TST in buildings

Power TBC

Downe Hospital:

7 ANPR mounted on columns soft digs

2 ANPR mounted on columns hard dig

5 TST

Ards Community Hospital:

8 ANPR on a new camera column soft dig

2 ANPR on a new camera column hard dig

4 ANPR wall mounted

6 desk mounted TST

Lagan Valley hospital:

4 ANPR Wall mounted

5 ANPR on a new camera column soft dig

5 ANPR on a new camera column hard dig

6 desk mounted TST

Ulster Hospital:

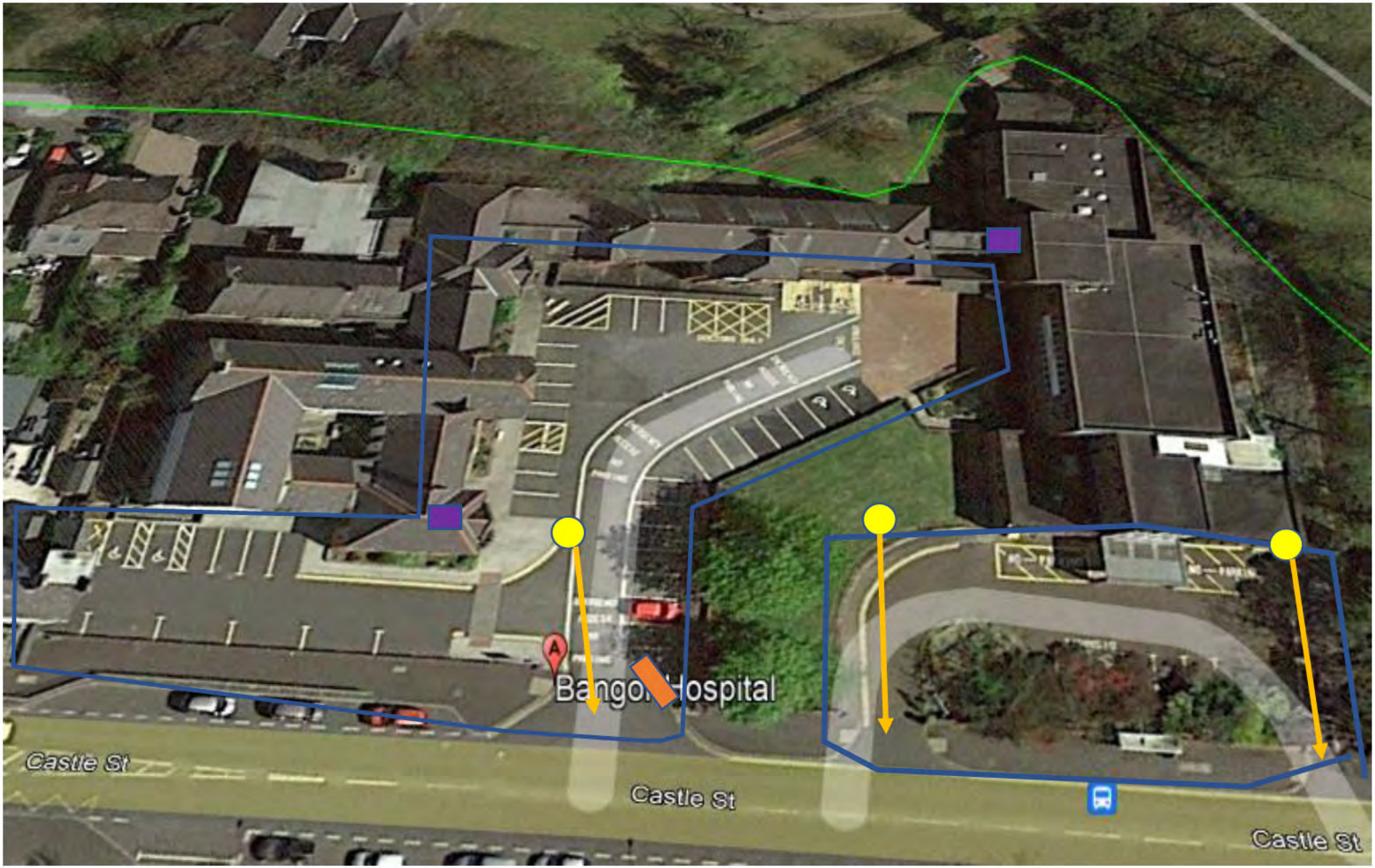
14 ANPR on a new camera column soft dig

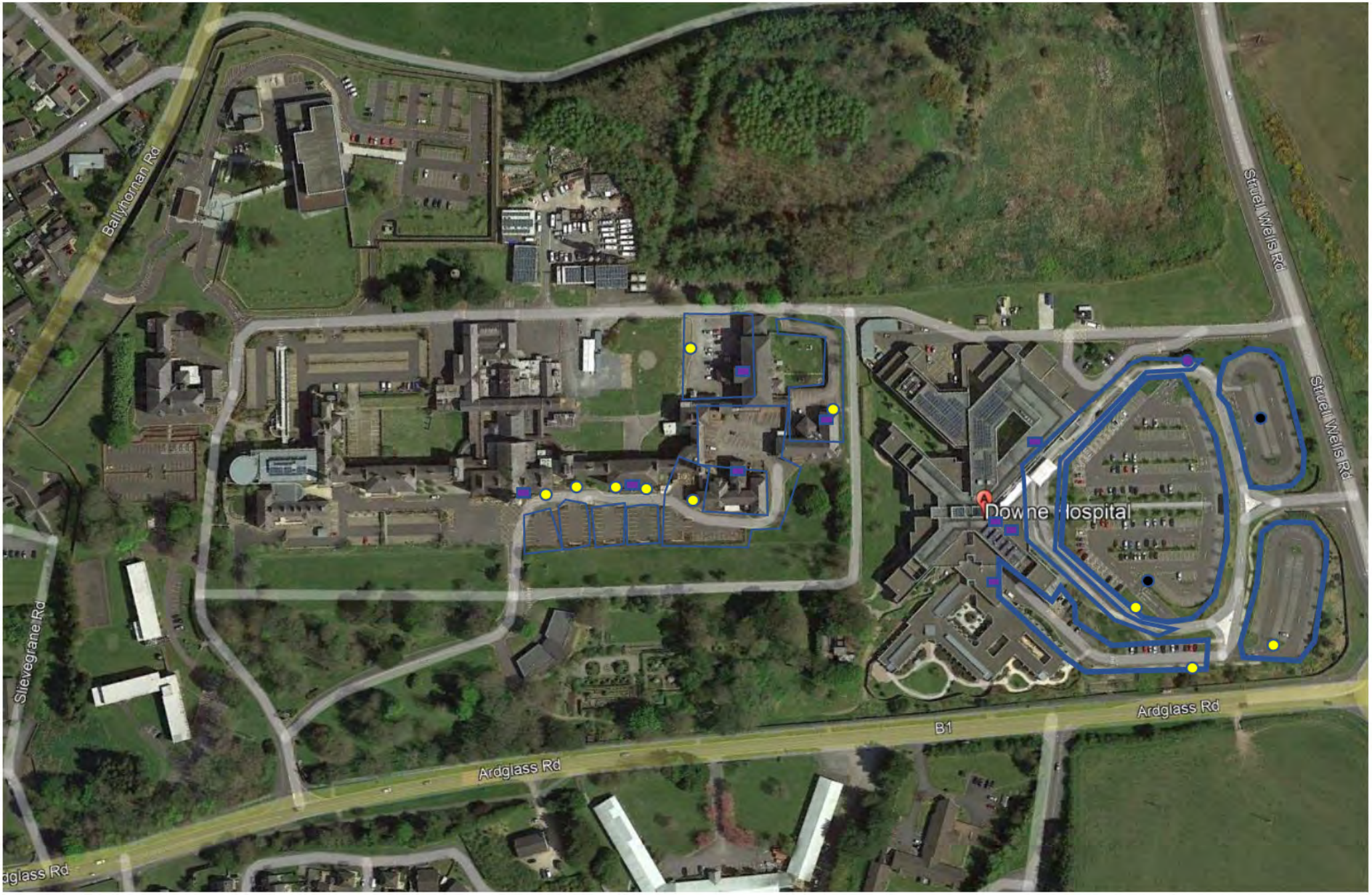
4 ANPR on a new camera column hard dig

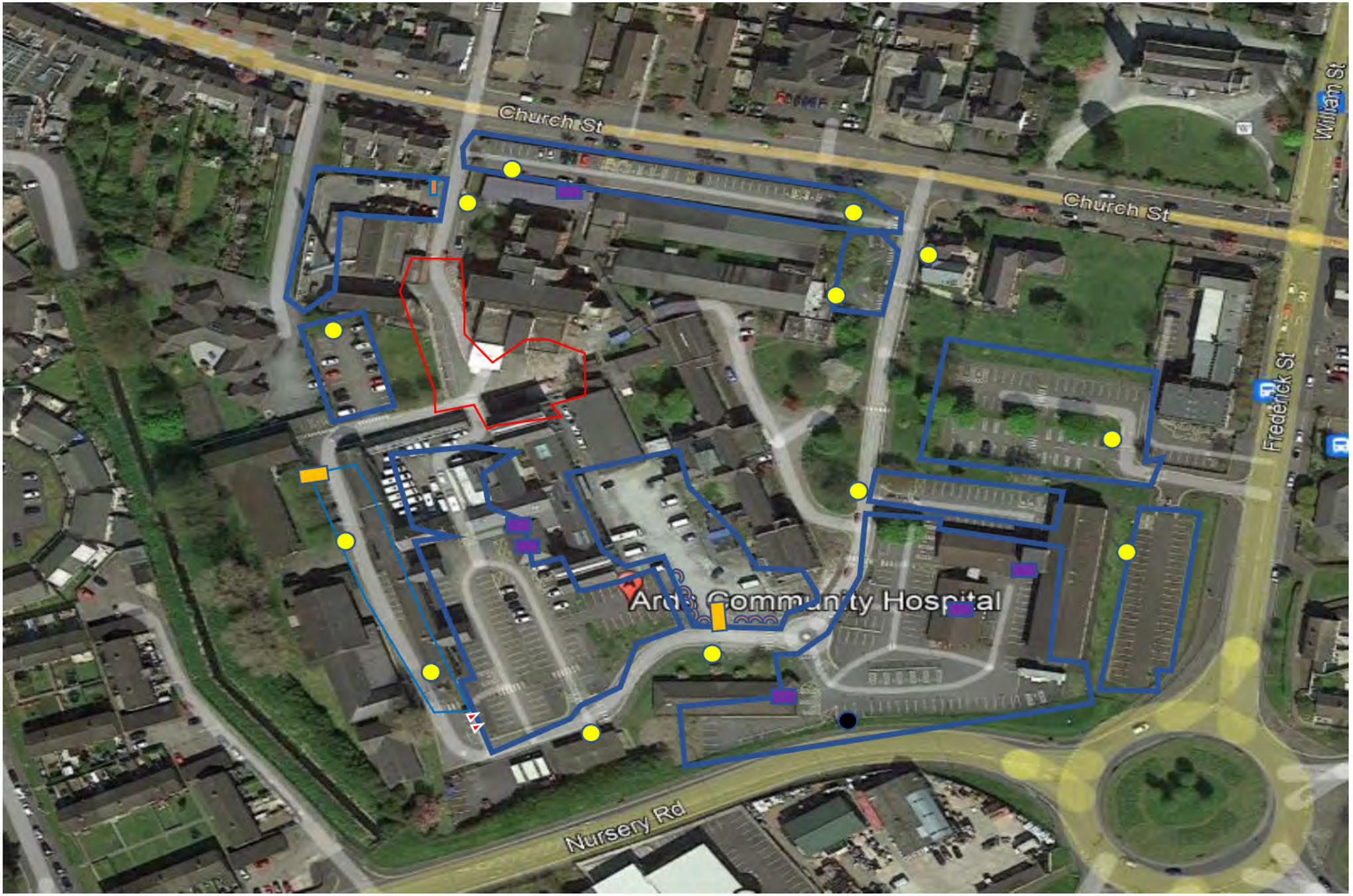
9 ANPR wall mounted

2 ANPR on existing poles

10 desk mounted TST


Castle St
Castle St
Castle St

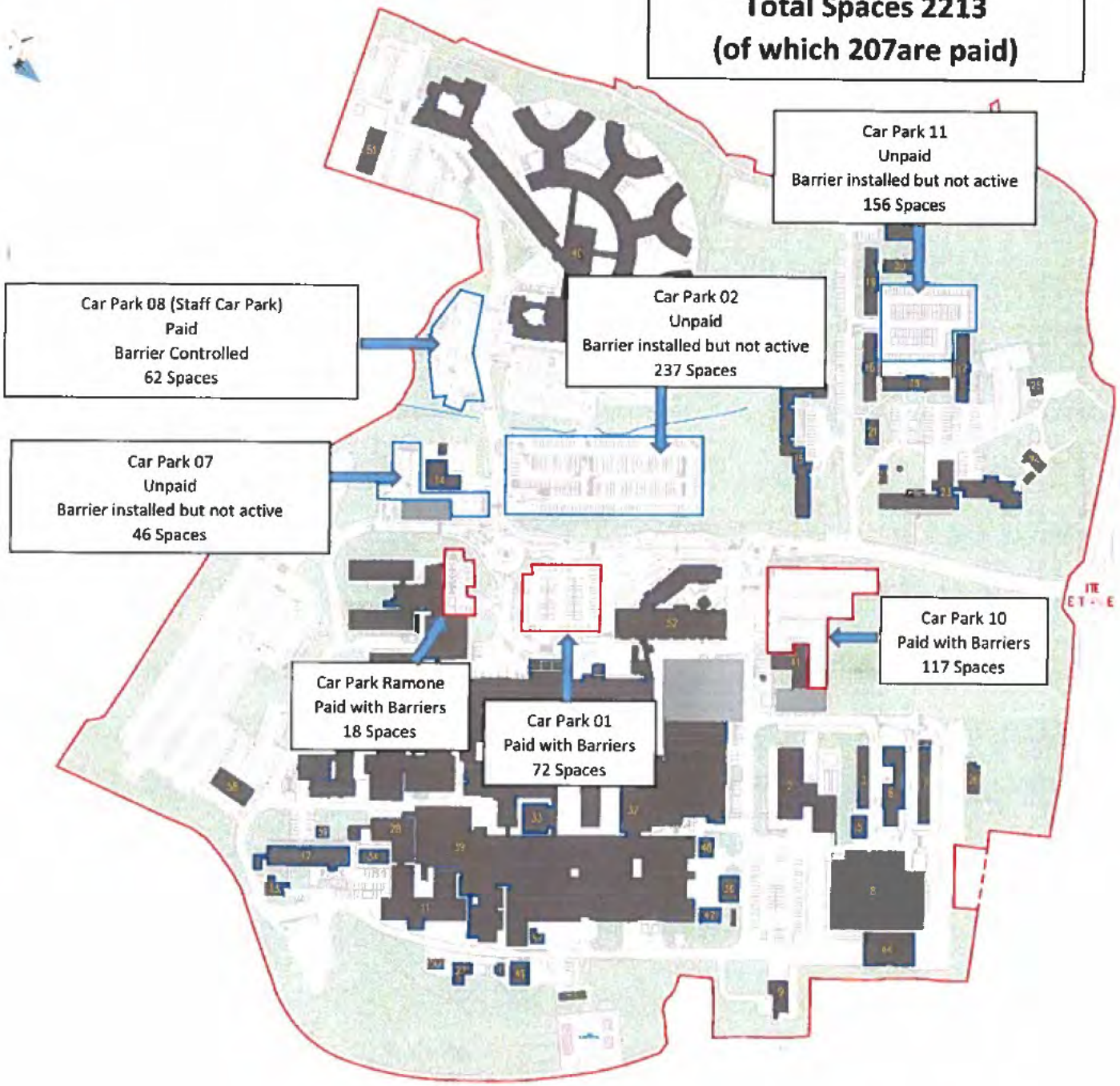

Ballyhornan Rd
Struell Wells Rd
Struell Wells Rd
Downe Hospital
Ardglass Rd
B1
Ardglass Rd
Slievegrane Rd
dglass Rd


Church St
Church St
William St
Frederick St
Nursery Rd

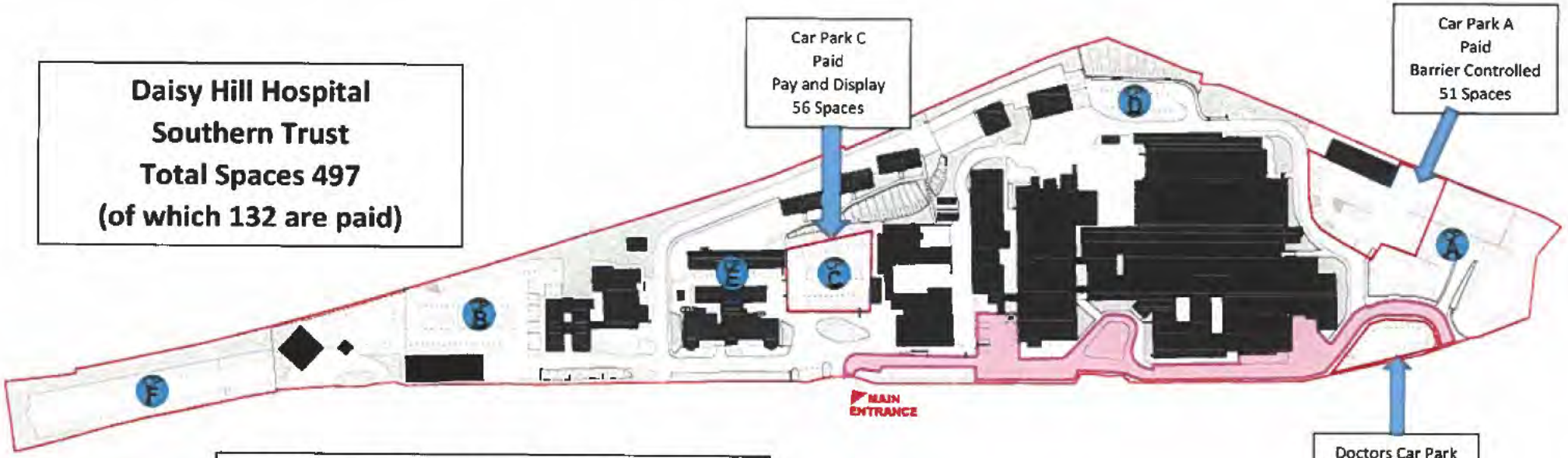

Lagan Valley Hospital
A1
Elmwood Dr


10
TST
Ulster Hospital

Craigavon Area Hospital
Southern Trust
Total Spaces 2213
(of which 207are paid)



Daisy Hill Hospital
Southern Trust
Total Spaces 497
(of which 132 are paid)



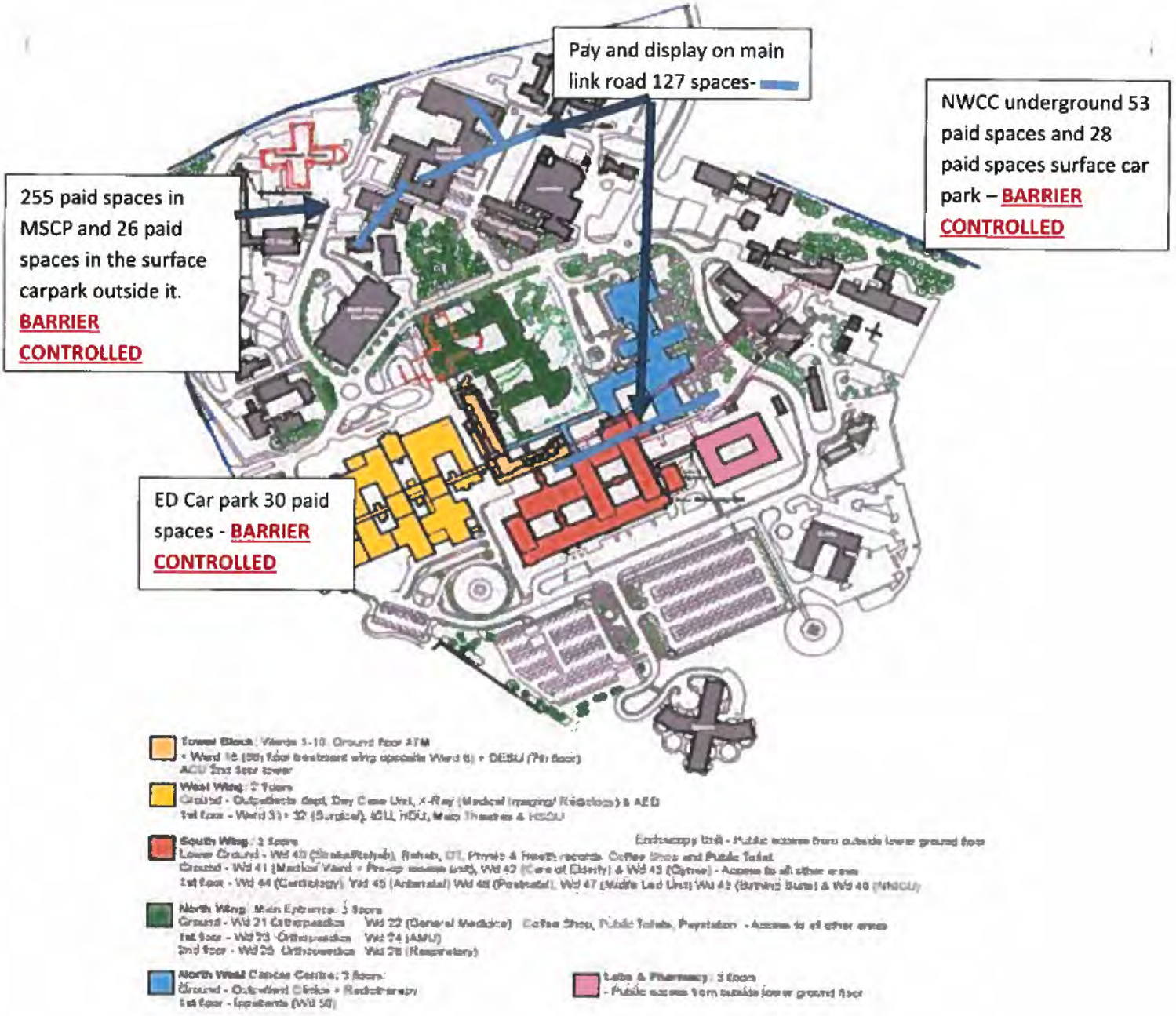
Car Park A – General use car park. Paid with barrier control.

Car Park C – There are no barriers to the car park. Payment is by pay and display only.

Doctors Car Park – This is a prepaid staff car park which is barrier controlled.

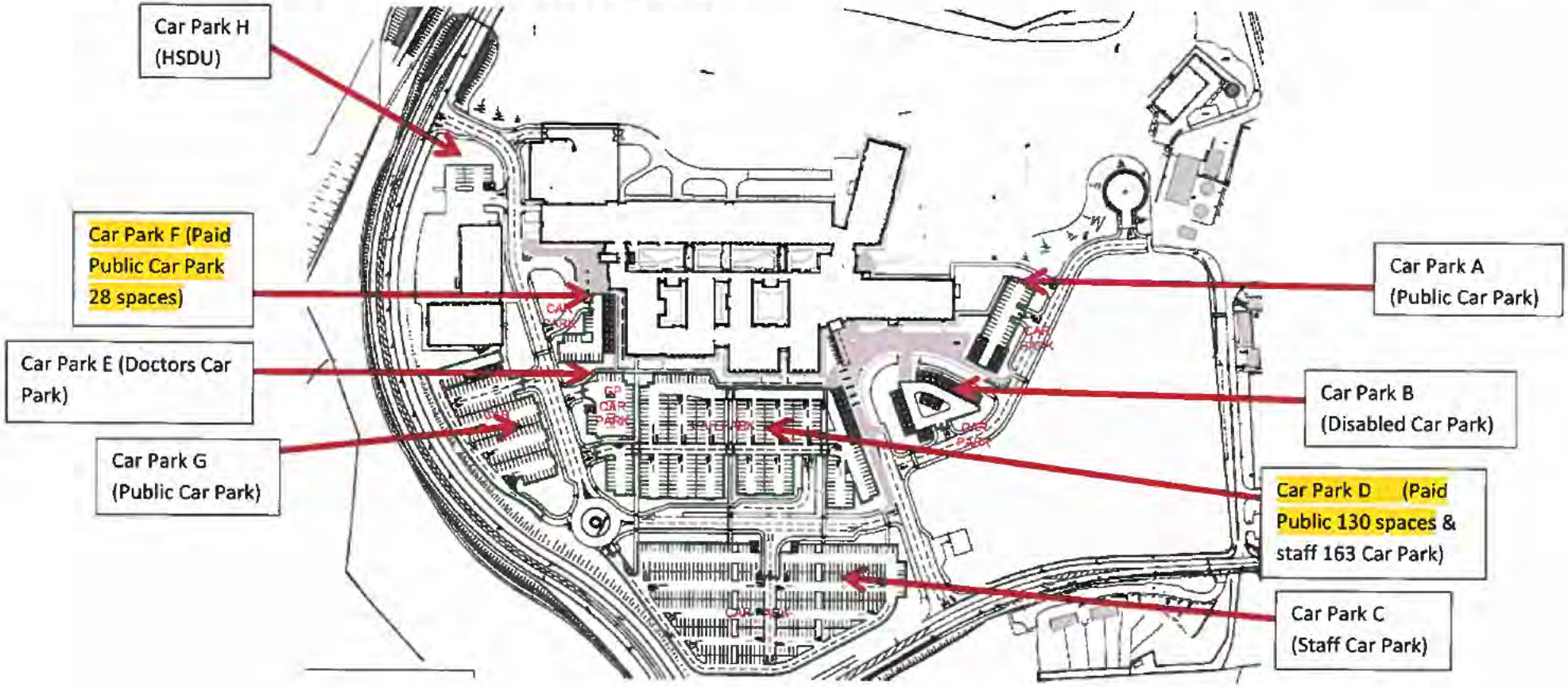
Altnagelvin Acute Hospital – Western HSC Trust.
Total of 2200 car parking spaces with 520 paid spaces across both barrier controlled car parks and ring road pay and display areas.

Altnagelvin Site Map

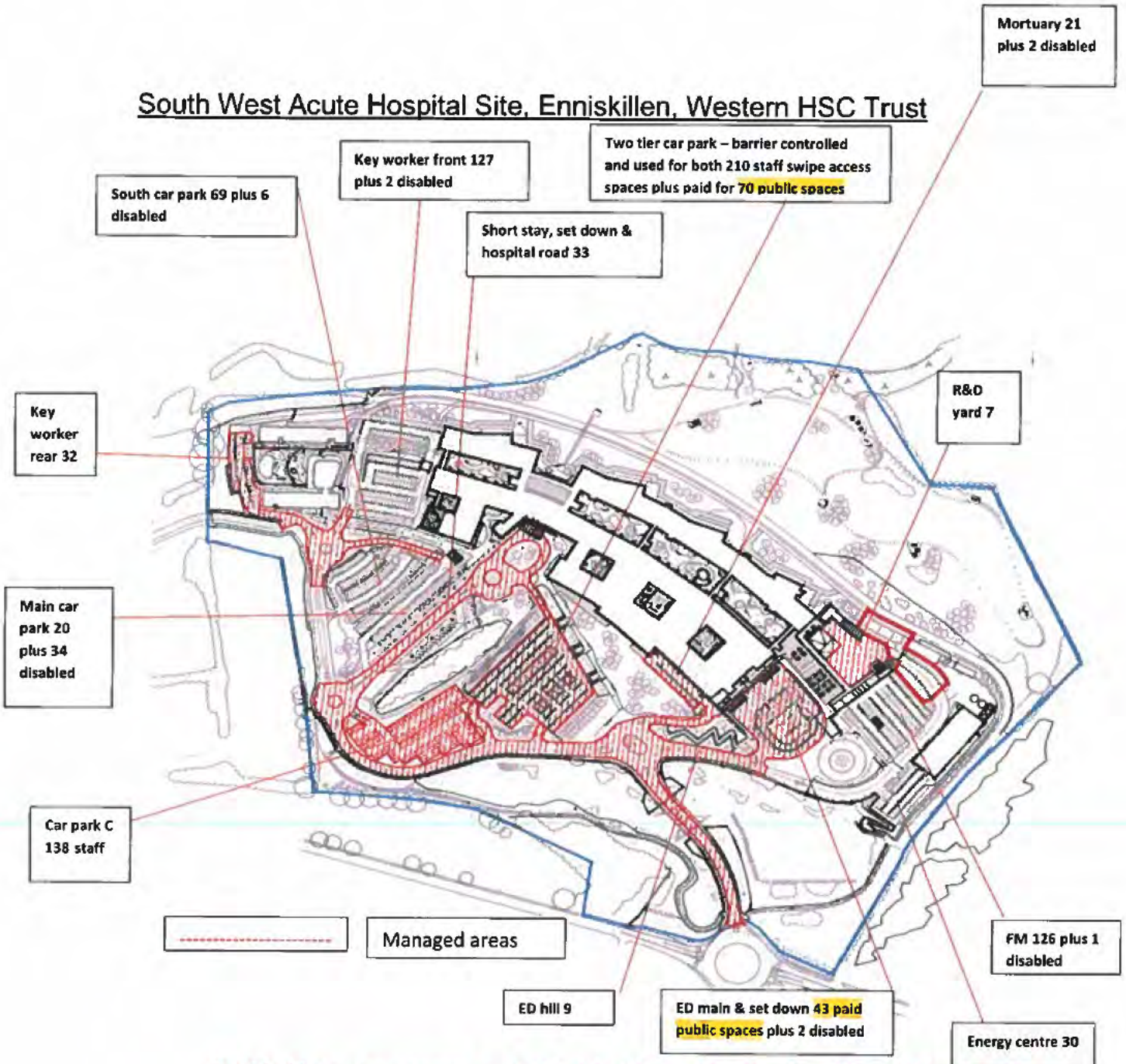


Omagh Hospital and Primary Care Complex Site Map

Local enhanced hospital and primary care site – non acute site with 2 continuing care wards, urgent care and treatment centre, cardiac assessment unit, 4No GP Surgeries, Renal Unit and significant level of Trust community and secondary care services –eg, Medical Imaging, Consultant Out Patient Clinics, Children's Centre etc. All paid parking spaces are barrier controlled.



South West Acute Hospital Site, Enniskillen, Western HSC Trust



Disabled bays, grass verges and all hatched boxes/ loading bays/drop off bays will be managed in all managed and non-managed areas.

Total spaces 990 of which 47 are disabled spaces

HSC SECURITY MANAGEMENT SCHEDULE

(LOW AND MEDIUM RISK)

1. SECURITY VETTING

1.1 All Contractor Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

1.2 The Authority and the Contractor shall review the roles and responsibilities of the Contractor Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Client Data or data which, if it were Client Data, would be classified as OFFICIAL-SENSITIVE.

1.3 The Contractor shall not permit Contractor Personnel who fail any security checks to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

1.4 The Contractor shall ensure that Contractor Personnel are only granted such access to Client Data as is necessary to enable the Contractor Personnel to perform their role and to fulfil their responsibilities.

1.5 The Contractor shall ensure that Contractor Personnel who no longer require access to the Client Data (e.g. they cease to be employed by the Contractor or any of its Sub-contractors), have their rights to access the Client Data revoked within 1 Working Day.

1.6 The Contractor shall ensure that Contractor Staff that have access to the Sites, the IT Environment or the Client Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Client Data.

1.7 The Contractor shall ensure that any training provided to Contractor Staff includes training on the identification and reporting fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the IT Environment or the Client Data (“phishing”).

2. INFORMATION GOVERNANCE

2.1 The Contractor shall ensure that the Services enable the Client to fulfil its responsibilities for information governance, including but not limited to the Client's responsibilities under the following pieces of legislation:

- [Official Secrets Act 1989;
- Public Records Acts 1958 and 1967;
- Data Protection Act 2018;
- UK General Data Protection Regulation;
- Freedom of Information Act 2000;
- Human Rights Act 1998;
- Computer Misuse Act 1990;
- Copyright (Computer Programs) Regulations;
- Civil Evidence Act 1968 and the Police and Criminal Evidence Act 1984;
- Regulation of Investigatory Powers Act 2000 (RIPA);
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; and
- The Communications Act 2003].

3 SECURITY CLASSIFICATION OF INFORMATION

3.1 If the provision of the Services requires the Contractor to Process Client Data which is classified as OFFICIAL-SENSITIVE, the Contractor shall implement such additional measures as agreed with the Client from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

4 RIGHT TO AUDIT

4.1 Without limitation to any other information governance requirements set out in these terms and conditions, the Contractor shall fully cooperate with any health checks, audits or investigations relating to information security and any privacy impact assessments undertaken by the Authority and shall provide full information as may be reasonably requested by the Authority in relation to such audits, investigations and assessments.

5 END USER DEVICES

5.1 The Contractor shall ensure that any Client Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority except where the Authority has given its prior written consent to an alternative arrangement.

5.2 The Contractor shall ensure that any device which is used to Process Client Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/collection/end-user-device-security.

6 NETWORKING

6.1 The Contractor shall ensure that any Client Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

7 IDENTITY, AUTHENTICATION AND ACCESS CONTROL

7.1 The Contractor shall operate an access control regime to ensure:

(a) all users and administrators of the Contractor System are uniquely identified and authenticated when accessing or administering the Services; and

(b) all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

7.2 The Contractor shall apply the 'principle of least privilege' when allowing persons access to the Contractor System and Sites so that such persons are allowed access only to those parts of the Sites and the Contractor System they require.

7.3 The Contractor shall retain records of access to the Sites and to the Contractor System and shall make such record available to the Authority on request.

8 DATA DESTRUCTION OR DELETION

8.1 The Contractor shall:

(a) prior to securely sanitising any Client Data or when requested the Contractor shall provide the Authority with all Client Data in an agreed open format;

(b) have documented processes to ensure the availability of Client Data in the event of the Contractor ceasing to trade;

(c) securely erase in a manner agreed with the Authority any or all Client Data held by the Contractor when requested to do so by the Authority;

(d) securely destroy in a manner agreed with the Authority all media that has held Client Data at the end of life of that media in accordance with any specific requirements in this Contract and, in the absence of any such requirements, as agreed by the Authority; and

(e) implement processes which address the CPNI and NCSC guidance on secure sanitisation.

9 AUDIT AND PROTECTIVE MONITORING

9.1 The Contractor shall collect audit records which relate to security events in the Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Contractor audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Client Data.

9.2 The Contractor and the Authority shall work together to establish any additional audit and monitoring requirements for the Information Management System.

9.3 The retention periods for audit records and event logs must be agreed with the Authority.

10 LOCATION OF CLIENT DATA

10.1 The Contractor shall not and shall ensure that none of its Sub-contractors Process Client Data outside the United Kingdom or the EU without the prior written consent of the Authority, which may be subject to conditions.

11 VULNERABILITIES AND CORRECTIVE ACTION

11.1 The Authority and the Contractor acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Authority Data.

11.2 The severity of vulnerabilities for COTS Software shall be categorised by the Contractor as ‘Critical’, ‘Important’ and ‘Other’ by aligning these categories to the appropriate vulnerability scoring systems including:

(a) the ‘National Vulnerability Database’ ‘Vulnerability Severity Ratings’: ‘High’, ‘Medium’ and ‘Low’ respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and

(b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

11.3 The Contractor shall procure the application of security patches to vulnerabilities in the Information Management System within:

(a) seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical';

(b) thirty (30) days after the public release of patches for those vulnerabilities categorised as 'Important'; and

(c) sixty (60) days after the public release of patches for those vulnerabilities categorised as 'Other'.

11.4 The timescales for applying patches to vulnerabilities in the Information Management System shall be extended where:

(a) the Contractor can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Contractor within agreed timescales if the vulnerability becomes exploitable within the context of the Services;

(b) the application of a 'Critical' or 'Important' security patch adversely affects the Contractor's ability to deliver the Services in which case the Contractor shall be granted an extension to such timescales of five (5) days, provided the Contractor had followed and continues to follow the security patch test plan agreed with the Authority; or

(c) the Authority agrees a different maximum period after a case-by-case consultation with the Contractor.

11.5 The Supplier shall ensure all COTS Software be kept up to date such that all COTS Software are always in mainstream support throughout the Contract Period unless otherwise agreed by the Authority in writing. All COTS Software should be no more than N-1 versions behind the latest software release.

12 SECURE ARCHITECTURE

12.1 The Contractor shall design the Information Management System in accordance with:

(a) the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;

(b) the NCSC "Bulk Data Principles", a copy of which can be found at https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and

(c) the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:

(i) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(ii) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

(iii) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(iv) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Contractor should have a security governance framework which coordinates and directs its management of the Services and information within it;

(v) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(vi) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Contractor Personnel have access to Client Data and/or the Client System that those personnel be subject to appropriate security screening and regular security training;

(vii) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

(viii) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Contractor to ensure that appropriate security controls are in place with its Sub-contractors and other Contractors;

(ix) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Contractor to make the tools available for the Authority to securely manage the Authority's use of the Service;

(x) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Contractor to

implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(xi) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;

(xii) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;

(xiii) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Contractor to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Client Data held by the Contractor and/or its Sub-contractors; and

(xiv) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Contractor to educate Contractor Personnel on the safe and secure use of the Information Management System.

Health and Social Care

Northern Ireland Fire & Rescue Service

HSC Supplier Security Policy

Approval

Document Reference	HSC Supplier Security Policy
Version	1.0
Last updated	31 October 2022
Owner	HSC Cyber Programme
Approval by	

Contents

1. DEFINITIONS

“Third Party” means any business partner, supplier, contractor, sub-contractor, reseller, distributor, joint venture, consortium, teaming partner, law firm or other business partner that will assist HSC in delivering services.

“HSC Information System” means any information system owned or controlled by HSC and used to store, process, transmit, or receive HSC Information. It also means any patient information systems or acquired services to the extent such information systems or services are physically or logically connected to HSC Information Systems or owned, controlled, managed or supervised by HSC organisations. Including the associated operating systems, applications and databases, either open-source or vendor provided.

2. INTRODUCTION

In entrusting its information and assets to external third parties HSC requires assurance that their integrity is maintained at every point in the supply chain, and those requirements are defined in the HMG Security Policy Framework (SPF). In addition there are also legal compliance requirements defined in the Data Protection Act 2018 (GDPR).

This policy document and the standards from which it is derived addresses the security assurance requirements in the contract management lifecycle. It applies to, and is intended for use by all HSC bodies, Northern Ireland Fire and Rescue Service (NIFRS) and their contracted staff (third party suppliers) engaged in supporting HSC and NIFRS services.

The requirements set out in this document are intended to support everyone involved in secure delivery of contractual obligations. In meeting these requirements it will assist HSC in achieving and maintaining ISO 27001 certification by mandating the information security controls required to meet Section A.15 of that standard. Effective information security is achieved by implementing a suitable set of controls to ensure that the specific security objectives of HSC are met. The data and information that HSC information systems contain, with particular regard to patient and client based data, must only be seen by those who are entitled to see it on a “Need to know basis”.

Health and Social Care in Northern Ireland are provided as an integrated service. There are a number of organisations who work together to plan, deliver and monitor Health and Social care across Northern Ireland.

3. PURPOSE

This policy sets out the requirements expected of third parties in order to effectively protect HSC information. This policy will ensure that HSC complies with its statutory duties laid out in the Data Protection Act 2018.

It will ensure that all third party organisations who enter into an agreement or contract with the HSC organisations are clear about the requirements in terms of information security and confidentiality.

It will ensure that all parties acting as a data processor for HSC will have the relevant technical and security measures in place to meet data protection legislation and privacy requirements.

The correct application of this policy will ensure that HSC is compliant with its legislative responsibilities, reduce the risk of an information security breach taking place and provide assurance to our staff and patients that information assets are being properly managed.

4. SCOPE

The scope of this policy is any third party which will process or have access to any HSC Information or information systems. This includes, but is not limited to:

- Third Party suppliers involved in the design, development and/or operation of information systems for any HSC organisation, writing and installing bespoke software, contractual support arrangements or operation of systems.
- Access to HSC information from remote locations where the computer and network facilities are not under the control of HSC
- Third parties who are not employees of any HSC organisation and require access to HSC information or information systems
- Access to HSC information via non-HSC applications and systems, which are hosted external to the HSC Network.

5. SECURITY ASSURANCE FOR THIRD PARTIES

A standardised process and framework for managing ICT contracts is used by HSC. Disclosure of HSC Information to third parties or access to HSC Information Systems shall not take place unless adherence to the HSC Cyber Security Assurance Framework is evidenced by third parties.

New ICT Contracts to HSC

New ICT contracts will be risk assessed using the HSC Cyber Supplier Risk Assessment Questionnaire (see APPENDIX B – REFERENCES). This will take place pre-procurement. The Service will return the completed questionnaire to the HSC body carrying out the compliance piece. This response will then be scored to determine one of four different Risk Profiles for the contract, each Risk Profile having a corresponding set of ICT security requirements.

Included in these requirements are a security accreditation requirement, where the chosen third party will self-certify that they have (or can commit to obtain, prior to the commencement of the contract) ICT Security certification that covers the scope required for all aspects of the contract, and that they commit to maintaining this standard for the duration of the contract. Third parties will also be expected to adhere to an HSC Security Management Schedule, this HSC Supplier Security Policy, and the HSC Network Code of Connection.

In addition, third parties may be subject to a "right to audit" clause by the procuring organisation, as set out in contract, and will fully cooperate with any audits or investigations.

Depending on the risk level associated with the contract, a request for evidence of any IT Health Checks carried out in the previous 12 months; or an IT Health Check performed by a CHECK Service Provider and/or an onsite security audit undertaken by the procuring organisation or their designated representative, may be made.

Risk Profiles

N/A – Requires no additional ICT security requirements beyond the standard T&Cs of the contract.

LOW – Cyber Essentials (self-certified) certification, HSC Security Management Schedule (Low and Medium Risk), this HSC Supplier Security Policy and the HSC Network Code of Connection.

MEDIUM – Cyber Essentials Plus certification, HSC Security Management Schedule (Low and Medium Risk), this HSC Supplier Security Policy and the HSC Network Code of Connection. Evidence of an IT Health Check carried out in the previous 12 months.

HIGH – Cyber Essentials Plus or ISO 27001 certification, HSC Security Management Schedule (High Risk), this HSC Supplier Security Policy and the HSC Network Code of Connection. An IT Health Check performed by a CHECK Service Provider, at the behest of the procuring organisation.

Security Assurance Review Outcome

All relevant information security requirements shall be established and agreed upon with each third party that will access, process, store, or communicate HSC Information, or provide HSC with IT infrastructure components that process HSC information. Legacy contracts that have been assessed as high risk by HSC Security, are to be brought into compliance with this standard upon renewal. All other legacy contracts are to be brought into compliance with this standard on a commercially reasonable effort.

6. SUPPLY CHAIN SECURITY MANAGEMENT

To maintain the confidentiality, availability, and integrity of HSC Information Systems, security requirements in service agreements with third party suppliers that deliver services or products to HSC and access HSC Information Systems as part of the delivery, shall be implemented.

Prior to their engagement, third parties may be subject to an independent, risk based due diligence evaluation. Information security requirements to mitigate the risks associated with a third party's access to HSC Information and Information Systems shall be agreed upon and documented as part of the final third party contractual agreement covering provision of third party's products and services.

7. RESPONSIBILITIES

Third parties providing products and services must confirm their compliance with the baseline security standards and obligations outlined in this security policy, to ensure appropriate measures have been taken and are in place to assure the continued security of the product or service provided.

The HSC supply chain and partners that we share data with have a responsibility to provide appropriate and continued protection for the full life span of any information shared. This extends to any further authorised sharing undertaken with another party with whom the Supplier enters into a Sub-contract. Third parties and partners are responsible for ensuring HSC requirements are passed down to those parties.

8. DATA PROTECTION AND PRIVACY

The third party organisation shall ensure compliance with all applicable laws and regulations relating to the processing of data and privacy protections. The current UK legal requirement for the lawful and correct handling of personal data is set out in the Data Protection Act 2018. This Act makes provision for the regulation of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information. Third parties shall comply with the requirements of this legislation at all times. Any non-compliance shall be notified in accordance with the HSC incident management process.

The third party shall ensure accuracy and completeness of controls to ensure the integrity of the information or information processing provided.

9. DATA CLASSIFICATION

HSC information is classified in terms of its value, legal requirements, sensitivity and criticality to the organisation. Each HSC organisation's Data Classification Policy contains direction on:

- Defining information;
- Classifying information;
- Accepting ownership for classified information;
- Labelling classified information;
- Storing and handling classified information;
- Managing network security;
- Categorising and labelling Personally Identifiable Information according to its sensitivity; and
- Making distinctions between ordinary personal data and special categories of personal data as required

10. DATA PROCESSING AGREEMENTS

The HSC Data Access Agreement Template can be found in Appendix B.

11. CALDICOTT PRINCIPLES

The following principles, drawn from the Caldicott Report 2013, must be upheld in respect of the holding and passing on of patient or client information to organisations within and outside the HSC.

1. Justify the purpose(s) for using confidential information.
2. Only use it when absolutely necessary.
3. Use the minimum that is required.
4. Access should be on a strict need-to-know basis.
5. Everyone must understand his or her responsibilities.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality

12. DATA PRIVACY IMPACT ASSESSMENTS

If personal data will be involved, a Data Privacy Impact Assessment must be undertaken by the Service, in conjunction with the third party, to understand the risk to the HSC data and to ensure GDPR is complied with. Guidance on DPIAs can be found here.

13. THIRD PARTY SYSTEMS SUPPORTING HSC

Development, test, and production facilities processing HSC Information must be separated to reduce risks of unwanted changes or unauthorised access to live HSC data. Live patient Information must not be used in development or test facilities.

14. THIRD PARTY ROLES AND RESPONSIBILITIES

Conflicting duties and areas of responsibility must be segregated to reduce opportunities for unintentional or unauthorised modification or misuse of HSC information.

15. THIRD PARTY PERSONNEL SECURITY

Security Screening, Confidentiality agreements and the prevention of terminated employees from accessing HSC Information and disciplinary measures for employees who violate information security policies and standards shall be in place.

15.1. SECURITY TRAINING

All Supplier Staff that have the ability to access HSC Information or Information Systems shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority / HSC in writing, this training must be undertaken annually.

15.2. THIRD PARTY MOVERS AND LEAVERS

HSC shall be informed immediately when a third party employee or sub-contractor with any HSC account is terminated from their employment or no longer supports HSC.

16. INFORMATION SECURITY MANAGEMENT SYSTEM

Operating procedures for information security management and controls related to HSC Information must be documented, maintained and made available to users involved in accessing or processing HSC Information and systems.

17. DEFINITION OF A SECURITY INCIDENT

The NCSC defines a cyber-incident as a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990).

In general, types of activity that are commonly recognised as being breaches of a typical security policy are:

1. Attempts to gain unauthorised access to a system and/or to data.
2. The unauthorised use of systems for the processing or storing of data.
3. Changes to a systems firmware, software or hardware without the system owners consent.
4. Malicious disruption and/or denial of service.

18. BUSINESS CONTINUITY AND DISASTER RECOVERY

All third party organisations must ensure that they develop and maintain business continuity and disaster recovery plans, based on business impact and risk assessments, to maintain adequate levels of HSC services in the event of any significant disruption to facilities or information services. These processes should be developed, tested and maintained in conjunction with data owners to ensure they are sufficient to provide an adequate level of service and recovery time.

19. CHANGE CONTROL FOR THIRD PARTY SERVICES

Changes to the provision of services by third parties, including maintaining and improving existing information security policies, procedures and controls, shall be managed, based on the criticality of business information, systems, and processes involved and re-assessing risks. HSC must be informed in advance of any proposed changes that could impact the CIA of HSC data or information systems. All changes will be subject to a security assessment, which may require an amendment to the contract.

20. SUB-CONTRACTING OF SERVICES

A Sub-contractor is any third party with whom:

(a) The Supplier enters into a sub-contract; or

(b) A third party under (a) above enters into a sub-contract, or the servants or agents of that third party.

21. CLOUD COMPUTING

Only shared hosting or As A Service (aaS) services that have been subject to an independent, risk based due diligence evaluation in accordance with the HSC Cloud Security Policy shall be used. HSC Information shall not be shared or stored with a hosting or aaS third party unless the security controls required by the contract or agreement are in place.

Before HSC Information is transferred for storage or processing to a shared hosting or aaS third party, the Supplier shall provide evidence that they protect the hosted environment and HSC Information as required by the contract or agreement and commensurate with the security categorisation of the HSC Information, as required by the HSC Cloud Security Policy.

22. COMPLIANCE

Any Supplier who violates this policy may be disabled from continued use/access to HSC, until a full investigation is complete.

APPENDIX A – LIST OF ORGANISATIONS

Strategic Planning and Performance Group (SPPG)

Public Health Agency (PHA)

Northern Health and Social Care Trust (NHSCT)

Southern Health and Social Care Trust (SHSCT)

South Eastern Health and Social Care Trust (SEHSCT)

Western Health and Social Care Trust (WHSCT)

Belfast Health and Social Care Trust (BHSCT)

NI Ambulance Service (NIAS)

Business Services Organisation (BSO)

Patient & Client Council (PCC)

Regulation & Quality Improvement Authority (RQIA)

NI Guardian Ad Litem Agency (NIGALA)

NI Blood Transfusion Service (NIBTS)

NI Social Care Council (NISCC)

NI Practice and Education Council for Nursing and Midwifery (NIPEC)

NI Medical and Dental Training Agency (NIMDTA)

GP Practices

NI Fire & Rescue Service (NIFRS)

And other Independent Contractors to HSC.

APPENDIX B - REFERENCES

Reference	Title	Location
Ref A	HSC Information Security Policy	HSC Information Security Policy
Ref B	HSC Network Code of Connection	HSC Network Code of Connection
Ref C	HSC Data Access Agreement	Data Access Agreement (v4.0)
Ref D	Third Party Access Request Form	Third Party Access Request Form
Ref E	Statement of Compliance Form for Third Parties	Compliance for Third Parties
Ref F	HSC Cyber Supplier Risk Assessment Questionnaire	HSC Cyber Supplier RAQ

Business Services Organisation
Providing Support to Health and Social Care

Revised 09/11/2023

Tender Number	4565034
Contract Title	Car Parking Solution Incorporating Automatic Number Plate Recognition and Enforcement
Company Name	

Pricing Schedule

Instructions to Tenderers

The following information is to assist you with your Tender submission.

Follow all instructions in full and only complete cells highlighted in yellow.

Prices must include all elements of the Scoping and Specification SS20a.

The figures in the blue cells will be automatically calculated, the figure in the total cell must be inserted when requested in the financial envelope.

Tenderers must enter a price against each line.
Tenderers must bid with only one price per line. Prices bid must be in GBP and to 2 decimal places.

Prices must be fixed for the first 12 Months of Contract.
Tenderers must ensure that all bid prices and calculations are accurate and correct.
These are estimated annual usage values, these values are a guide only and are not deemed to be a condition of the Contract or a guarantee of minimum demand or uptake.
This information is given for guidance only. No compensation will be payable to the Contractor should the actual demand be less than that stated.

The prices bid below is for the overall products and service as detailed in the Scoping and Specification SS20a.

Details on the installation and dig requiements can be found in point 3.2 Installation, Project Management and Commissioning of the Scoping and Specification SS20a Revised 09/11/2023.

Please complete the VAT Rate column using the key below. Please input as follows:
ST - if you are obliged to pay the standard VAT rate 20%
00 - if you are not obliged to invoice for VAT in the UK
EX - if you are VAT exempt

Refer to the Tender Evaluation Methodology and Marking Scheme (TEMMS) SS20b document for details on how price will be evaluated.

Section B is for information only and will not be evaluated but will form part of the Contract

Section A - Product and Service Requirements

Product Description	Estimated Usage	UOM	Unit Price	Total Cost	VAT Rate	Brand	Product Name and Code	Lead Time
ANPR System - Hard Dig - Supply, install and commission For evaluation purposes the pole will be 8 metres 1200mm planting depth; Dig shoud be per 5m run.	100	each		0.00				
ANPR System - Soft Dig - Supply, install and commission For evaluation purposes the pole will be 8 metres 1200mm planting depth; Dig shoud be per 5m run.	100	each		0.00				
ANPR System - Wall Mounted - Supply, install and commission; the brackets suitable for the camera supplied. For evaluation purposes the camera must be situated at 8 metres from ground.	96	each		0.00				
Signage - Hard Dig - Supply and install For evaluation purposes the pole will be 8 metres 1200mm planting depth.	100	each		0.00				
Signage - Soft Dig - Supply and install For evaluation purposes the pole will be 8 metres 1200mm planting depth.	100	each		0.00				
Signage - Wall Mounted - Supply and install For evaluation purposes the sign must be situated at 8 metres from ground.	96	each		0.00				
Touch Screen Terminals - Indoor	90	each		0.00				
Touch Screen Terminals - Outdoor	45	each		0.00				
Hand Held Devices and Printers for ticketing	30	each		0.00				
Patrol Wardens (37.5 hours per week)	39 000	per hour		0.00				
Issuing of PCNs	40 157	each		0.00				
Annual Maintenance of all equipment and signage from year 2	1	per annum		0.00				
Annual fee for access to portal and reporting and full support managing all PCNs revenue collection, appeals and notices of court action	1	per annum		0.00				
			Total	**0.00**				

Section B - Additional Costs - for information only, will not be evaluated but will form part of the Contract

Product Description	UOM	Unit Price	VAT Rate	Brand	Product Name and Code	Lead Time
ANPR System on pole and hard dig - Supply install and commission	each					
ANPR System, on pole and soft dig - Supply, install and commission	each					
ANPR System wall mounted - Supply install and commission	each					
Patrol Wardens for out of hours	per hour					
Training of Patrol Wardens including accreditations	per participant					
Call out fee for repairs	per hour					
Consumables for the hand held devices and printers, please list any additional consumables below						

Tender Evaluation Methodology and Marking Scheme (TEMMS)

Tender Number:	4565034
Contract Title:	Car Parking Solution Incorporating Automatic Number Plate Recognition and Enforcement
Period of Contract:	Five Years from the date stated on the Award Letter with provision to extend for up to and including 36 Months

Introduction

This document outlines the evaluation methodology and the marking scheme in terms of scoring and weightings that will be applied to this Tender.

This process seeks to establish a Contract awarded to a sole supplier.

The Contract Adjudication Group (CAG) will evaluate the Tender submissions. This Tender contains three (3) envelopes as listed below, and these are referred to in the relevant steps of the evaluation process:

- Eligibility Envelope
- Technical Envelope
- Financial Envelope

Clarifications (during the Tender advert period)

Should clarification be required on any aspect of the information published, clarification questions must be submitted in writing via the eTendersNI portal before the closing date for receipt of clarifications. Questions and responses will, in most cases, be made available to all Tenderers.

The closing date for receipt of clarifications is 15:00 Friday 10 November 2023.

Evaluation Process Steps

This Tender will be checked and evaluated as detailed in the following steps of the evaluation process.

Step 1: Compliance Checks

There are a number of compliance checks which will be carried out during the various steps of the evaluation process. These are as follows:

- All Tender submissions will be checked to ensure that each Tender is compliant in that it has been submitted in accordance with the notes and instructions stated within the various envelopes.
- All Tender submissions will be checked to ensure that Tenderers have attached the SS19a Pricing Schedule and have bid for all lines.

Tenderers who have met all of the compliance checks within a particular step will have their Tender progressed within the evaluation process.

If a Tenderer fails a compliance check within an envelope, then in accordance with the notes or instructions within the envelope, they may have their Tender deemed as non-compliant and may have their Tender rejected at that step.

Step 2: Exclusion Grounds (Eligibility Envelope)

The eligibility envelope contains a number of questions relating to exclusion grounds. These questions will be evaluated as detailed in **Table 1 – Exclusion Grounds** below.

Only Tenderers who have achieved a full pass rate in all of the exclusion grounds questions will progress to the selection criteria evaluation.

Reference	Exclusion Grounds	Evaluation Methodology
Q18.1 Mandatory Exclusions	Compliance with Regulation 57 (1) and 57 (2)	**Pass or Fail** A "No" statement will result in a pass. A "Yes" statement will result in a fail unless evidence is provided at Q18.2 to demonstrate reliability in accordance with Regulation 57 (13) (self-cleaning) to the satisfaction of the Authority.
Q18.3 Mandatory and Discretionary Exclusions for Non-Payment of Taxes etc.	Compliance with Regulation 57 (3)	**Pass or Fail** A "No" statement will result in a pass. A "Yes" statement will result in a fail unless evidence is provided at Q18.4 to demonstrate the fulfilment of obligations in accordance with Regulation 57 (5).
Q18.5 Mandatory and Discretionary Exclusions for Non Payment of Taxes etc.	Compliance with Regulation 57 (4)	**Pass or Fail** A "No" statement will result in a pass. A "Yes" statement will result in a fail unless evidence is provided at Q18.6 to demonstrate the fulfilment of obligations in accordance with Regulation 57 (5).

Reference	Exclusion Grounds	Evaluation Methodology
Q18.7 Discretionary Exclusions	Compliance with Regulation 57 (8)	**Pass or Fail** A "No" statement will result in a pass. A "Yes" statement will result in a fail unless evidence is provided at Q18.8 to demonstrate reliability in accordance with Regulation 57 (13) (self-cleaning) to the satisfaction of the Authority.

Table 1 – Exclusion Grounds

Step 3: Selection Criteria (Eligibility Envelope)

The eligibility envelope contains a number of questions relating to selection criteria. These questions will be evaluated as detailed in **Table 2 – Selection Criteria** below.

Reference	Selection Criteria	Evaluation Methodology
Section 19 Economic and Financial Standing	Q19.1 Bankers details	**Pass or Fail** To achieve a pass, you must provide the information requested, otherwise fail.
	Q19.2 Banking History	**Pass or Fail** To achieve a pass, you must provide the information requested, otherwise fail.
	Q19.4 Statement of Accounts Please provide your last two years financial accounts.	**Pass or Fail** To achieve a pass, you must provide your last two years financial accounts as requested and achieve an acceptable evaluation of your audited account by a competent financial advisor chosen by the Client, otherwise fail.

Reference	Selection Criteria	Evaluation Methodology
	Q19.5 Independent Financial Check	**Pass or Fail** To achieve a pass, you must confirm your acceptance to an independent financial check of your audited accounts, otherwise fail.
Q20 Technical and Professional Ability	Q20.1 Previous Experience Tenderers must provide a detailed example of having provided a similar Service to the scope and scale of this Tender within the last 3 years. The example provided must include the following information: - Contract name / organisation name - Contract start and completion date (if applicable) - Annual value - Details of similar Service provided.	**Pass or Fail** To achieve a pass, you must answer the question in full detailing all relevant current and previous experience to the scope and scale of this Contract, otherwise fail.

Table 2 – Selection Criteria

Only Tenderers who have achieved a full pass rate in all of the selection criteria questions will progress to the award criteria evaluation.

Step 4: Award Criteria

The Contract will be awarded based on the following award criteria – most economically advantageous Tender, in terms of the weightings as described in the table below.

Award Criteria	Weighting
Quality	Pass or Fail
Quality – Non-Price Scored Questions	60%
Social Value Considerations	Pass or Fail
Social Value Considerations	10%
Price	30%
Total	**100%**

Step 4a: Award Criteria – Non-Price (Eligibility Envelope and Technical Envelope)

The eligibility and technical envelopes contain a number of award criteria questions. These questions will be evaluated as detailed in **Table 3 – Award Criteria – Non-Price** below.

Reference	Award Criteria	Evaluation Methodology (Scoring and Weighting)
Award Criteria (Eligibility Envelope) Only Tenderers who have achieved a full pass rate in all questions/criteria will progress further in the process.		
Q21.1	Tenderers must confirm that they can provide all elements of the Scoping and Specification SS20a.	**Pass or Fail** A "yes" response is a pass. A "no" response is a fail.
Q21.2	Tenderers must provide evidence that they are a member of the BPA Approved Operator Scheme.	**Pass or Fail** To achieve a pass, Tenderers must attach evidence that they are a member of the BPA Approved Operator Scheme, otherwise fail.
Q21.3	Tenderers must confirm they have achieved a cyber essentials certification or they will achieve this by the Contract Commencement Date, and will maintain the certification for the life of the Contract.	**Pass or Fail** A "yes" response is a pass. A "no" response is a fail.

Reference	Award Criteria	Evaluation Methodology (Scoring and Weighting)
Q21.4	Tenderers must state their compliance with Appendix 6 – HSC Security Management Schedule.	**Pass or Fail** A "yes" response is a pass. A "no" response is a fail.
Q21.5	Tenderers must state their compliance with Appendix 7 – HSC Supplier Security Policy.	**Pass or Fail** A "yes" response is a pass. A "no" response is a fail.
Award Criteria – Quality (Technical Envelope) A pass mark of 45% out of 60% has been set for the total score against the award criteria. Only Tenderers whose total percentage weighted score is equal to or greater than the pass mark will progress to the next step in the Tender evaluation.		
Technical Envelope, Q1.1	This question requires Tenderers to detail how they will provide and meet the following elements as detailed in the Scoping and Specification SS20a document. • ANPR System - points 2.2.1 and 2.2.2 • Patrol Wardens / Civil Parking Enforcement - points 2.5, 2.5.1 and 2.5.2 • PCN Issue and Processing – point 2.6 This is an attachment question and the response must be no more than 8 sides of an A4 page and should be in Arial font, size 12.	**36%** Please refer to Table 4 – Evaluation Rationale
Technical Envelope, Q1.2	This question requires Tenderers to provide an implementation plan and a timeline meeting all elements as	**12%** Please refer to Table 4 – Evaluation Rationale

Reference	Award Criteria	Evaluation Methodology (Scoring and Weighting)
	detailed in point 3, 3.1 and 3.2 of the Scoping and Specification SS20a document. This is an attachment question and the response must be no more than 4 sides of an A4 page and should be in Arial font, size 12.	
Technical Envelope, Q1.3	This question requires Tenderers to detail how they will provide Customer Support meeting all elements as detailed in points 7, 7.1, 7.2 and 7.3 of the Scoping and Specification SS20a document. This is an attachment question and the response must be no more than 3 sides of an A4 page and should be in Arial font, size 12.	**6%** Please refer to Table 4 – Evaluation Rationale
Technical Envelope, Q1.4	This question requires Tenderers to detail how they will provide Maintenance meeting all elements as detailed in point 9 of the Scoping and Specification SS20a document. This is an attachment question and the response must be no more than 3 sides of an A4 page and should be in Arial font, size 12.	**6%** Please refer to Table 4 – Evaluation Rationale

Reference	Award Criteria	Evaluation Methodology (Scoring and Weighting)
Award Criteria – Social Value Considerations (Technical Envelope) A pass or fail question has been set for social consideration question 2.1 and a pass mark of 4% out of 10% has been set for this social consideration question 2.2. Only Tenderers who pass question 2.1 and whose score is equal to or greater than the pass mark for question 2.2 will progress to the next step in the Tender evaluation.		
Technical Envelope, Q2.1	Tenderers must attach the completed Social Value Delivery Plan. Tenderers must only complete cells highlighted in yellow, any additional information included within the Social Value Delivery Plan will not be evaluated as part of the Tender return.	**Pass or Fail** To achieve a pass, Tenderers must attach the Social Value Delivery Plan identifying the minimum indicative points as per Annex A, otherwise fail.
Technical Envelope, Q2.2	Tenderers must detail how they will deliver the Social Value Initiatives within their completed Social Value Delivery Plan as outlined in Schedule 4 in the Scoping and Specification SS20a and Annex A of this document. This is an attachment question and the response must be no more than 3 sides of an A4 page and should be in Arial font, size 12.	**10%** Please refer to Table 4 – Evaluation Rationale

Table 3 – Award Criteria – Non-Price

Eligibility Envelope

Award criteria questions in this envelope are pass or fail. Tenderers must pass all award criteria questions, within the eligibility envelope otherwise your Tender will fail and your bid will not be considered any further in the evaluation process.

Technical Envelope

Award criteria questions in this envelope are weighted as per Table 3 and scoring will take place as per **Table 4 – Evaluation Rationale**, below.

Responses to the questions above require an attachment for each question. These attachments must not exceed the page limit as stated. Any additional characters / words exceeding the specified number above will be disregarded and will not be evaluated or scored as part of the Tender response. Diagrams, graphs, charts and CVs will not contribute to the page limit for these questions. Responses must not include reference to URL's, cross referencing, embedded files, since these will be disregarded and will not be evaluated or scored as part of the Tender response.

Mark	Description
0	Failed to address the question / issue / Specification.
1	An unacceptable response to the Specification/answer/solution with serious reservations. Limited detail of the methodology to be applied. High risk that the proposed approach will not be successful.
2	A response to the Specification/answer/solution with reservations. Lacks convincing detail of the methodology to be applied. Medium risk that the proposed approach will not be successful.
4	Meets Requirements. The response to the Specification/answer/solution generally meets the requirements, but lacks sufficient detail to award a higher mark.
5	Excellent response that meets the requirements of the Specification/answer/solution. Indicates an excellent response with detailed supporting evidence and no weaknesses. Response demonstrates that this Contractor will provide outstanding goods and Services if awarded.

Table 4 – Evaluation Rationale

For clarification purposes please note – there is no mark 3 in the above table.

Step 4b: Award Criteria – Price (Financial Envelope)

All Tenderers must follow the instructions detailed in the financial envelope and the Pricing Schedule SS19a. It is the Tenderers responsibility to ensure the accuracy of the figures inserted against all lines. Prices must include all elements of the Specification. Prices must be fixed for the first 12 months of the Contract.

Section 1 - The estimated annual usage figure for each line will be multiplied by the bid price per Tenderer to calculate the total cost per line for each Tenderer. This total cost per line will be automatically calculated and the sum of all lines will be added together to give the overall total bid price that will be used in the calculation below.

Section 2 is for information only and will not be evaluated but will form part of the Contract.

The price weighted score (PWS) will be calculated as follows:

$$\text{PWS (\%)} = \frac{\text{Price of the lowest compliant Tender submitted}}{\text{Price of the Tender being assessed}} \times 30\%$$

This will allow each Tenderer to achieve a percentage score, calculated to two decimal points. The model above will award 30% to the lowest compliant tendered price and pro-rata decreasing scores for all other Tender submissions. The price used will be the total sum of all priced elements as listed in the Pricing Schedule SS19a.

Step 5: Award of Contract

At this stage only the Tenderers who have successfully progressed through all steps detailed above will have their scores totalled.

It is intended to make award of Contract to the highest scoring Tenderer.

In instances where Tenderers achieve the same overall score and there is a tie break situation, the Tenderer with the highest % score in Non-Price scored questions will be awarded the Contract.

Tender Validity Period

Tenders MUST remain open for the period stated in the eTendersNI portal ("the Tender Validity Period" (TVP)). The Contracting Authority may request that Tenderers extend the TVP for specified additional period(s) as may reasonably be requested. Where a Tenderer confirms they do not agree to extend the TVP (or any previous extension of the TVP) that Tenderer's Tender may be excluded.

Annex A

Award Criteria

In accordance with the Procurement Policy Note (PPN) 01/21 (Scoring Social Value Policy), the Contractor will be required to deliver measurable social value outcomes.

As outlined in Schedule 4 of the SS20a Scoping and Specification, the Contractor must provide social value to a minimum value of 100 social value points for every £1 million (and pro-rata) of the invoiced value, capped at an averaged invoiced value of £3 million per annum**. For the purposes of evaluation, Tenderers should submit their responses based on a minimum indicative value of 630 social value points.**

Tenderers are required to complete and submit with their Tender response the Social Value Delivery Plan (excel spreadsheet) identifying which Social Value Initiatives they will deliver to fulfil the minimum indicative 630 social value points and answer the following question:

How will you deliver the Social Value Initiatives within your completed Social Value Delivery Plan as outlined in Schedule 4.

Tenderer Guidance

Your response must address the following:

- Timescales for delivery of the social value requirements;
- The resources, both internal and external, you will use to plan and deliver the social value requirements (this should include details of suppliers in your supply chain);
- The activities you will undertake to deliver the social value initiatives selected within your completed Social Value Delivery Plan, including how you will engage with key stakeholders (including communities impacted through the delivery of the contract);
- Confirmation that the planned activities are additional to activities your organisation already undertakes; and,
- How you will monitor and report on the delivery of the social value requirements and address any performance issues.

Your response should be no more than 3 sides of one A4 page and should be in Arial font, size 12.

Please note, the Social Value Delivery Plan (excel spreadsheet) must be completed and submitted as part of your Tender response. Tenderers must only complete the cells highlighted in yellow within the Social Value Delivery Plan. Any additional information included by Tenderers within the Social Value Delivery Plan <u>will not</u> be evaluated as part of your Tender response.