SCHEDULE 13

Data Processing and Information Security

Part 1
Data Processing and Contact Details

1. The contact details of the Authority's Data Protection Officer is: dataprotectionofficer@sheffield.gov.uk

2. The contact details of the Operator's Data Protection Officer (or equivalent contact) is: [redacted]

3. In accordance with clause 53.3.2.1, where the Operator is acting as a Processor, the Operator shall comply with any further written instructions from the Controller with respect to processing. Any such further instructions shall be notified from time to time by the Authority's Data Protection Officer (acting reasonably, having due regard to the nature of the data and whether the Authority is, in respect of such Personal Data, a Controller).

Part 2
Information Security

1. **Security standards**

The Operator shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

1.1 is in accordance with applicable Legislation and this Agreement;

1.2 as a minimum, demonstrates Good Industry Practice;

1.3 complies with the Protective Measures set out in paragraph 3; and

1.4 meets any specific known security threats which pose an immediate and high risk to Personal Data.

2. **Security Management Arrangements**

2.1 **Introduction**

2.1.1 The Operator shall maintain Security Management Arrangements which will be in line with the requirements of this part 2 of schedule 13 (*Data Processing and Information Security*).

2.1.2 The Operator shall thereafter comply with its obligations set out in the Security Management Arrangements.

2.2 **Content of the Security Management Arrangements**

2.2.1 The Security Management Arrangements shall:

2.2.1.1 comply with the principles of security set out in paragraph 1 and any other provisions of this Agreement relevant to security of information;

2.2.1.2 identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Operator;

2.2.1.3 detail the process for managing any security risks arising from the use of Sub-Contractors (including Processors and Sub-processors) and third parties with access to:

(a) Personal Data;

(b) processes associated with the Personal Data and any ICT, information and data (including the Authority's Confidential Information and the Personal Data); and

(c) any system that could directly or indirectly have an impact on that Personal Data; and

2.2.1.4 set out the security measures to be implemented and maintained by the Operator in relation to all aspects of the Personal Data and all processes associated with the provision of the Services and shall ensure that the Contract Management System complies with the provisions of this Agreement.

2.3 **Review of the Security Management Arrangements**

2.3.1 The Security Management Arrangements shall be fully reviewed and updated by the Operator at least annually to reflect:

2.3.1.1 emerging changes in Good Industry Practice;

2.3.1.2 any change or proposed change to the Personal Data and/or associated processes;

2.3.1.3 any new perceived or changed security threats; and

any local variations required by this paragraph 2.3.1 to the Operator's information security management system shall be reflected in the Business Continuity Plan as the case may be.

2.3.2 The Operator shall provide the Authority an outline of:

2.3.2.1 the results of such reviews; and

2.3.2.2 any proposed amended Security Management Arrangements upon reasonable request at no additional cost to the Authority

2.3.3 Any change or amendment which the Operator proposes to make to the Security Management Arrangements (as a result of a review carried out in accordance with paragraph 2.3.1) shall be compliant with the provisions of paragraph 2.2.

2.3.4 The reviewed and amended Security Management Arrangements outlined to the Authority in accordance with paragraph 2.3.2, will thereafter be adopted and will replace the previous version of the Security Management Arrangements and thereafter operated and maintained in accordance with part 2 of this schedule 13.

2.3.5 The Authority shall be entitled to comment on the outlined Security Management Arrangements pursuant to paragraph 2.3.4 and the Operator shall act reasonably and have due regard to any suggestions, but shall have no obligation to adopt any changes to the Security Management Arrangements.

2.3.6 Submission of the Security Management Arrangements pursuant to paragraph 2.3.4 shall not relieve the Operator of its obligations under this schedule 13 (*Data Processing and Information Security*).

3. **Protective Measures**

In accordance with clause 55.4.3.1 of the Agreement, the Operator shall ensure that it has in place Protective Measures which are appropriate to protect against a Data Loss Event, including the following (save that, where the following protective measures can not be directly implemented due to system limitations or architecture, the Operator may use their discretion to implement compensating controls to reduce the risk):

3.1 the Operator shall ensure that any site or other location used to Process Personal Data will have suitable physical security controls and shall provide the Authority with a copy of the Operator's physical security policy, together with an explanation of its physical security processes;

3.2 the Operator shall put in place, maintain and shall provide the Authority with copies of appropriate information security and data security policies that are conformant to relevant and proportionate industry standards, together with a staff awareness programme;

3.3 the Operator shall put in place and maintain a formal incident response process which is specific to information security events. Any incidents which may have a material direct, or indirect, impact on Personal Data relevant to the Authority must be reported immediately to the Authority through its information security incident reporting process;

3.4 the Operator shall ensure that any system or network Processing Personal Data meets the requirements of UK GDPR;

3.5 where a network is used by the Operator, the Operator shall ensure that the service is proportionately protected, irrespective of specific hosting requirements with regard to location (on premises or cloud). Where the Operator's systems are hosted by cloud suppliers, the underpinning principles of security remain true and should be suitably assured;

3.6 the Operator shall ensure that in relation to Personal Data, any and all:

3.6.1 staff;

3.6.2 persons performing any of the Services; and

3.6.3 persons that require access,

are duly Authorised and that any access to such Personal Data must conform to the principles of 'need to know' and 'least privilege' with robust controls in place to ensure Personal Data is not shared inappropriately;

3.7 the Operator must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified and authenticated as appropriate;

3.8 the Operator shall control access to Personal Data and maintain access policies including specific reference to remote access and bring-your-own-device policies;

3.9 the Operator must retain records of access to the physical data centre;

3.10 the Operator shall comply with the provisions of clause 60.1 and ensure that, where required by legislation, it has completed a valid disclosure check through the Disclosure and Barring Service of the most extensive available kind that is appropriate to the Personal Data that will be accessed for all relevnt members of staff involved in handling Personal Data;

3.11 the Operator shall ensure that all staff that have the ability to access Personal Data or systems holding Personal Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority in writing, this training must be undertaken annually;

3.12 the Operator shall run routine security testing of their infrastructure and services. This should be conducted by an independent CREST or other suitably accredited third party (as the case may be);

3.13 the Operator shall maintain vulnerable management and penetration testing processes and outline the process adopted for a network level penetration test to the Authority on request;

3.14 the Operator shall ensure that services that are presented to external networks (whether internal services accessed by staff or web services presented to the general public) are architected to ensure separation of functionality to adequately protected tiers and that external facing components are hosted in a separated DMZ;

3.15 the Operator shall maintain an assurance process which applies to third party suppliers, Sub-Contractors or any other party who may host or have access to the Operator's network or systems;

3.16 the Operator shall ensure that the CMS must support role based access controls. It must be possible to configure these to a sufficiently granular level to support the principle of least privilege. For example, the elevated privileges required for systems maintenance reasons should not necessarily grant access to all information. CMS users must only be able to view information, records or documents where applicable that they have entitlement to view or edit;

3.17 the Operator shall ensure that the CMS supports the principal of 'separation of duties'. For example, the system shall force separation of duties with respect to performing functions requiring access to sensitive data or multi step processes requiring authorisation;

3.18 the Operator shall ensure that the CMS shall support unique and identifiable logins, including an authentication system which requires passwords to meet a minimum configuration level in line with [Microsoft AD], including complexity rules, longevity and lock out capabilities;

3.19 the Operator shall ensure that any passwords or other authentication credentials stored by the CMS are stored in a manner that prevents them from being read, disclosed or otherwise compromised, for example salted password hashes;

3.20 where a backend portal (such as the CMS) is presented on the internet, the Operator shall ensure that MFA is mandatorily required for all users accessing the back end;

3.21 the Operator shall ensure that:

3.21.1 where passwords are used as the primary authentication method, the password issue/reset functions ensure that users are the only persons who have knowledge of their created password and no one else (not even helpdesk operators or system administrators) may know another user's password;

3.21.2 initial or reset passwords do not follow an easily guessed pattern; and

3.21.3 initial or reset passwords are not transferred via an insecure transport channel;

3.22 the Operator shall ensure that the CMS must demonstrably have been developed to mitigate the risks of cyber-attack including addressing the Open Web Application Security Project top 10 threats;

3.23 the Operator shall put robust controls in place to protect against the risk of receiving malicious code wherever a public facing portal provides the ability to upload files from an untrusted network or device. Controls may include but are not limited to: the ability to filter by file header information or other heuristic means rather than simply file extension and 'sheep dip' staged area approach to prevent passing of files directly to live system;

3.24 the Operator shall ensure that its system allows for the encryption of data in all states (at rest, in transit and during processing) and also in all elements of the system whether live or in backup;

3.25 the Operator shall ensure that the CMS supports secure web architecture and any public facing content input facility or functionality for serving internally generated web content to the public is designed to a recognised architectural pattern which does not expose backend components or internal network infrastructure directly, specifically, it must be possible to split and separate the presentation, business logic and data tiers so that they are hosted in separated network segments;

3.26 where the Operator uses third party hosting, management or any other service, the Operator shall apply adequate security policies, processes and auditing to such relationships;

3.27 the Operator shall ensure that Personal Data Processed or held in systems is stored in the UK;

3.28 the Operator shall implement agreed processes to ensure that:

3.28.1 any security incident, which may have either a direct or indirect impact on the Authority, is reported to the Authority immediately; and

3.28.2 anomalies and security events identified by the Authority can be reported to the Operator (including named roles and defined escalation routes);

3.29 the Operator shall ensure that its CMS is patchable and shall provide updates and patches to address security vulnerabilities and operational software bugs in a timely manner and shall support the installation of these updates in a manner that does not require the system to be re-installed or cause major operational disruption. This pertains to all elements of the CMS including client and server components and OS level dependencies. If the system is to become unsupported or no longer patchable in the future, the Operator shall ensure that there is a defined and supported upgrade path to a version which does fulfil this requirement;

3.30 the Operator shall ensure that its CMS has full audit trail functionality attributable to individual solution users, including:

3.30.1 successful login/logout;

3.30.2 unsuccessful login/logout;

3.30.3 unauthorised access (where applicable);

3.30.4 record or data access attempts;

3.30.5 actual and attempted data manipulation and modification; and

3.30.6 privileged system changes (for example account management, policy changes, device configuration);

3.31 the Operator shall ensure that the ability to set up and amend user accounts in its CMS is limited to authorised Operator staff;

3.32 the Operator shall collect audit records which relate to security events in delivery of the CMS or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Operator audit records should (as a minimum) include:

3.32.1 regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Personal Data;

3.32.2 logs to facilitate the identification of the specific asset which makes every outbound request external to the CMS (to the extent that the CMS is within the control of the Operator). To the extent the design of the CMS allows, such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers; and

3.33 the Operator and the Authority shall work together to establish any additional audit and monitoring requirements for the CMS;

3.34 the Operator must document and agree the retention periods for audit records and event logs with the Authority;

3.35 the Operator shall perform a technical information risk assessment on the Services and shall demonstrate what controls are in place to address those risks;

3.36 the Operator shall ensure that:

3.36.1 any Personal 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; and

3.36.2 any device which is used to process Personal Data meets all of the security requirements set out in the National Cyber Security Centre's End User Devices Platform Security Guidance published on 17 November 2018, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security;

3.37 the Operator must be able to demonstrate they can supply a copy of all Personal Data on request or on termination of the Services, and must be able to securely erase or destroy all Personal Data and media that the Personal Data has been stored and processed on; and

3.38 the Operator must ensure that all commercial off-the-shelf software and third party commercial off-the-shelf software be kept up to date such that all Operator software and third party software are always in mainstream support.