**Security Standards Agreement for A Support Service for Parents/Carers of Children and Young People Affected by or at risk of Extra-Familial Exploitation and/or who repeatedly go missing, in York and North Yorkshire (contract ref: 2324-0223)**

This agreement acts as a supplementary agreement to the **[Contract /Agreement, insert URN]** between the **[Name of Police Force/s],** hereinafter referred to as the Force(s), and **[Supplier or Partner Organisation],** hereinafter referred to as the Supplier. It establishes the security requirements that the Supplier shall comply with in provision of services to the Force/s.

The purpose of this agreement is to formally communicate the expectations that the Force/s, has regarding the Supplier handling of information relating to the **[insert project/contract title].** The standard of protection required varies with the sensitivity of the information being shared. The primary objective of this agreement is to ensure the appropriate handling of HMG/Policing information by the Supplier, and the correct allocation of classifications and their associated handling instructions to information related to the services generated by (and provided to) the Supplier relating to **[insert project/contract title].**

This agreement does not preclude the security responsibilities detailed in the **[Contract/Data Protection Contract, insert URN]** or to be detailed in the stated contract. This version of the agreement supersedes any previous versions issued.

**1. National Standards**

The Force handle all HMG/policing information in line with the following national standards:

* Security Policy Framework (SPF)[[1]](#footnote-1)
* Authorized Professional Practice on Information Management[[2]](#footnote-2)
* Guidance on the Management of Police Information (2nd Edition, 2010)[[3]](#footnote-3)
* The Authorised Professional Practice for Vetting[[4]](#footnote-4)
* PSN Code of Practice[[5]](#footnote-5)
* Government Security Classification (GSC)[[6]](#footnote-6)
* NCSC Data at Rest[[7]](#footnote-7)
* NCSC Secure Sanitisation of Storage Media[[8]](#footnote-8)
* NCSC Data in Transit Protection[[9]](#footnote-9)

And when a cloud service is been used:

* NCSC’s Cloud Security Principles[[10]](#footnote-10)

Note: These standards include all aspects of security and Information Management (data processing, communication, file classification, transmission, storage, retention and disposal). Not all the above national standards will be relevant to the **[insert project/contract title].** The Supplier must ensure it has adequate governance including organisational policies for security standards including technical, logical and administrative controls that adhere to the above standards or higher.

**2. Sub-Contractors/Processing and Off Shoring**

The Supplier must ensure that any sub-contractors/processing also adhere to the stated requirements via the same means.

Any Off Shoring will only be done with direct approval from the Force/s as detailed in the **[Contract /Agreement, insert URN].**

**3. Confidentiality and Non-disclosure of HMG/Police information**

The data processed in relation to the **[insert project/contract title]** could have a direct impact on operational policing, the effective working of the criminal justice system and potentially the security of the nation.

The Supplier’s attention is therefore drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 4 of the Official Secrets Act 1989. The Supplier shall take all reasonable steps to make sure that all individuals employed on any work in connection with the **[insert project/contract title]** have notice that these statutory provisions apply to them and shall continue to apply after the completion or earlier termination of this **[insert project/contract title].**

Staff of the Supplier may be required to sign a Force(s) Undertaking of Confidentiality/ Acknowledgment (UoC/A) and or data access agreements / remote access agreements as part of the **[Contract /Agreement, insert URN].**

**4. Government Security Classification**

All information provided under the GSC will be classed as **OFFICIAL** but will generally have no marking to identify it as **OFFICIAL**. The Force/s will label **OFFICIAL-SENSITIVE** as such.

**File Classification –** Suppliers own company policy/guidelines can be followed providing they are underwritten by current national standards, comparable with GSC and stand to regular review, audit and scrutiny.

OFFICIAL Examples

**Transmission –** Use of a technical solution may be acceptable subject to prior agreement with the Force’s Information security team. For mail it must be sent in the post or via a courier service, in a sealed envelope. Envelope must be fully addressed to the named recipient and include return address details. All technical transmissions and communications i.e. email, and file transfer solutions must use encryption standards AES 256 as minimum and TLS 1.2 protocols.

Below is a standards document that is followed by Police Forces:



**Remote Working -** Suppliers own company policy/guidelines can be followed providing information cannot be inadvertently overlooked whilst being accessed remotely. Force information should be adequately protected from unauthorised access, modification and loss at all times.

**Storage –** For physical storage information must be held under a single barrier and/or lock and key and access only granted to those with the appropriate employment checks and vetting and ‘need to know’. Digital data storage must be protected by infrastructure and a network protected by security in depth as directed by national guidance.

**Disposal –** Disposal is as per the guidance provided by NCSC with regards to [secure sanitisation of storage media](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media) and through their own policy/guidance.

OFFICIAL-SENSITIVE Examples

**Transmission –** All technical transmissions and communications i.e. email, and file transfer solutions must use encryption standards AES 256 as minimum and TLS 1.2 protocols. Use of a secure technical solution following the national standards above is acceptable e.g. a CJSM email address. For mail double enveloped. Do not show classification on the outer envelope. Label the inner envelope OFFICIAL-SENSITIVE. Both envelopes should be fully addressed to the named recipient and include return address details. Material must be sent via a service with the ability to track the material until the point of successful delivery to the intended location.

**Remote Working –** Only to be allowed if the Supplier has a company policy/guidelines and information cannot be inadvertently overlooked whilst being accessed remotely and assets used to process OFFICIAL-SENSITIVE information are secured via the appropriate technical and organisational measures as detailed in the national standards above.

**Storage –** For physical storage information must be held under two different barriers and/or lock and key and access only granted to those with the appropriate employment checks and vetting and have a ‘need to know’. Digital data storage must be protected by infrastructure and a network protected by security in depth as directed by national guidance.

**Disposal -** Disposal is as per the guidance provided by NCSC with regards to [secure sanitisation of storage media](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media).

This guidance is not exhaustive. If in doubt, the Supplier must contact the Force for clarity on the handling and storage of any information. A Handling Policing Data within OFFICIAL document is available on request.

**5. Actions**

You are requested to acknowledge receipt of this agreement and to confirm by signature (below) that the national standards stated in Section 1 have been brought to the attention of the person directly responsible for the security and information management of this project, that they are fully understood, and that the required technical and organisational security measures can and will be taken to safeguard the data concerned.

If you have any difficulty in interpreting the meaning of the above standards, please let Force(s) know.

Note: It is recommended that your organisations signs up to the Cyber Security Information Sharing Partnership (CiSP) run by the NCSC if your organisations has not already done so - [CiSP - NCSC.GOV.UK](https://www.ncsc.gov.uk/section/keep-up-to-date/cisp)

**5. Signatures**

*Sign Here*

**Signed on behalf of the Supplier[[11]](#footnote-11)**

**Date:**

*Sign Here*

**Force Accreditor(s)**

**Date:**

1. <https://www.gov.uk/government/publications/security-policy-framework> [↑](#footnote-ref-1)
2. <https://www.app.college.police.uk/app-content/information-management/> [↑](#footnote-ref-2)
3. <https://ict.police.uk/wp-content/uploads/2016/07/mopi-refreshed-guidance.pdf> [↑](#footnote-ref-3)
4. <http://library.college.police.uk/docs/appref/C666I0917-Vetting-APP-22.10.17.pdf> [↑](#footnote-ref-4)
5. <https://www.gov.uk/government/publications/psn-code-of-practice-cop> [↑](#footnote-ref-5)
6. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf> [↑](#footnote-ref-6)
7. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/882760/dwp-ss007-security-standard-use-of-cryptography-v1.1.pdf> [↑](#footnote-ref-7)
8. <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media> [↑](#footnote-ref-8)
9. <https://www.ncsc.gov.uk/guidance/tls-external-facing-services> [↑](#footnote-ref-9)
10. <https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles> [↑](#footnote-ref-10)
11. A board level member who has responsibility and accountability for Information Risk within the supplier’s organisation. [↑](#footnote-ref-11)