INFORMATION SHARING AGREEMENT

BETWEEN

THE CHIEF CONSTABLE OF NORTH YORKSHIRE POLICE

AND

THE YORK & NORTH YORKSHIRE COMBINED AUTHORITY

AND

PROVIDER

|  |
| --- |
| **SUMMARY SHEET** |

|  |  |
| --- | --- |
| **ISA Reference No:** |  |

|  |  |
| --- | --- |
| **PURPOSE:** | To create a system for the disclosure of:   * personal data and anonymised individual level data between the Policing, Fire and Crime Directorate of YNYCA, North Yorkshire Police and provider; * anonymised demographic data of those referred by North Yorkshire Police between North Yorkshire Police, YNYCA and provider; and * performance summary reporting with North Yorkshire Council and the City of York Council as co-commissioners of the services   with the intention to allow the Chief Constable for North Yorkshire and the YNYCA to meet their obligations to offer those affected by sexual violence appropriate support services to cope and recover under Code of Practice for Victims of Crime. |

|  |  |
| --- | --- |
| **PARTNERS TO THIS AGREEMENT:** | The Chief Constable, North Yorkshire Police  YNYCA  PROVIDER |

|  |  |
| --- | --- |
| **Date Agreement Comes Into Force:** | When Agreement has been signed by all Partners |

|  |  |
| --- | --- |
| **Date of Agreement Review:** | Initially after 6 months, then annually |

|  |  |
| --- | --- |
| **Agreement Owner:** | Sally Lynch, Commissioning and Partnerships Manager |

|  |  |  |
| --- | --- | --- |
| **Version Number** | **Amendments Made** | **Authorisation** |
|  |  |  |
|  |  |  |

Contents

[1. INTRODUCTION 5](#_Toc144479385)

[2. PURPOSE AND SCOPE OF THIS AGREEMENT 5](#_Toc144479386)

[3. AGREEMENT ADMINISTRATION 5](#_Toc144479387)

[3.1. Partners to the Agreement 5](#_Toc144479388)

[3.2. Commencement of the Agreement 6](#_Toc144479389)

[3.3. Withdrawal from the Agreement 6](#_Toc144479390)

[3.4. Review of the Agreement 6](#_Toc144479391)

[3.5. Audit Arrangements 7](#_Toc144479392)

[4. POWER OR DUTY TO SHARE INFORMATION 7](#_Toc144479393)

[5. LEGAL COMPLIANCE 8](#_Toc144479394)

[5.1. Duty of Confidence 9](#_Toc144479395)

[5.2. Data Protection Act 2018 and General Data Protection Regulations 10](#_Toc144479396)

[5.3. Human Rights Act 1998 11](#_Toc144479397)

[6. TYPES OF INFORMATION TO BE SHARED 11](#_Toc144479398)

[7. ROLES AND RESPONSIBILITIES 15](#_Toc144479399)

[8. PROCESS OF SHARING 16](#_Toc144479400)

[8.1. Access to the Information 16](#_Toc144479401)

[8.2. Sharing Procedure 16](#_Toc144479402)

[8.3. Ensuring the Accuracy of Information Shared 17](#_Toc144479403)

[8.4. Information Management 17](#_Toc144479404)

[8.5. Information Security 17](#_Toc144479405)

[8.5.1. Information Security Governance & Risk Management 18](#_Toc144479406)

[8.5.2. Access Control 18](#_Toc144479407)

[8.5.3. Security Architecture & Design 19](#_Toc144479408)

[8.5.4. Physical & Environmental Security 19](#_Toc144479409)

[8.5.5. Telecommunications & Network Security - nil 19](#_Toc144479410)

[8.5.6. Cryptography – nil 19](#_Toc144479411)

[8.5.7. Business Continuity & Disaster Recovery 19](#_Toc144479412)

[8.5.8. Legal, Regulations, Compliance & Investigations 19](#_Toc144479413)

[8.5.9. Software Development Security – nil 20](#_Toc144479414)

[8.5.10. Security Operations 20](#_Toc144479415)

[9. MISCELLANEOUS MATTERS 21](#_Toc144479416)

[9.1. Indemnity 21](#_Toc144479417)

[9.2. Access Rights of Data Subjects 21](#_Toc144479418)

[9.3. Freedom of Information Act Considerations 22](#_Toc144479419)

[10. SIGNATURES 22](#_Toc144479420)

# INTRODUCTION

Version:1.10.0.3

Hash:e/Yj9M3lIEOcgkXWAL3DquM2wOc=

This Agreement has been developed to:

* Document the specific purposes for which the Partners have agreed to share information;
* Describe the roles and structures that will support the exchange of information between Partners;
* Set out the legal gateway through which the information is shared, including any reference to the Data Protection Act 2018 and General Data Protection Regulations (“DPA/GDPR”), the Human Rights Act 1998 (“HRA”) and the Common Law duty of confidentiality;
* Describe the security procedures necessary to ensure compliance with legal and regulatory responsibilities including under the DPA/GDPR and any Partner specific security requirements;
* Ensure compliance with individual Partners’ policies, legal duties and obligations;
* Ensure that the Chief Constable for North Yorkshire Police complies with the Code of Practice on the Management of Police Information made under the Police Act 1996 and the Police Act 1997; and
* Ensure that the Chief Constable for North Yorkshire Police complies with the Information Commissioner’s Code of Practice on Data Sharing.

# PURPOSE AND SCOPE OF THIS AGREEMENT

The purpose of this Agreement is to facilitate the exchange of information to enable those directly affected by sexual violence to receive appropriate support services to cope and build resilience and to increase victim satisfaction and overall public confidence in the Criminal Justice System.

This Agreement will ensure that information is exchanged to meet this purpose in a way that is compatible with all Partners’ obligations under the DPA/GDPR and Human Rights Act 1998.

Sharing of information on a day-to-day basis under this Agreement will generally be undertaken by the individuals and methods described in Sections 6 and 7 of this Agreement.

# AGREEMENT ADMINISTRATION

## Partners to the Agreement

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Postal Address** | **Email Address** | **Telephone Number** |
| The Chief Constable for North Yorkshire Police | NYP Headquarters,  Alverton Court  Northallerton  DL6 1BF | officeofthechiefconstable@northyorkshire.police.uk | 01609 643 666 |
| Policing, Fire and Crime Directorate part of the York & North Yorkshire Combined Authority | Policing, Fire and Crime Directorate YNYCA,  Harrogate Police Station,  Beckwith Head Road,  Harrogate,  HG3 1FR | info@northyorkshire-pfcc.gov.uk | 01423 569 562 |
| PROVIDER | TBC | TBC | TBC |

## Commencement of the Agreement

This Agreement shall commence upon the signing of a copy of the Agreement by all Partners.

## Withdrawal from the Agreement

Any Partner may withdraw from this Agreement upon giving written notice to all other Partners. The Partner must continue to comply with the terms of this Agreement in respect of any information that the Partner has obtained through being a Partner to this Agreement. Information which is no longer relevant should be returned or destroyed in an appropriate secure manner as per 8.4.

## Review of the Agreement

In accordance with the requirements of the Code of Practice for the Management of Police Information, this Agreement will be reviewed six months after its implementation by the Chief Constable for North Yorkshire Police’s Single Point of Contact (“SPOC”) and annually thereafter.

The review will:

* Ensure the contact list at section 7 is up-to-date;
* Consider whether the Agreement is still useful and fit for purpose;
* Identify any emerging issues; and
* Determine whether the Agreement should be extended for a further period (up to one year) or whether to terminate it.

The decision to extend or terminate the Agreement and the reasons for this decision will be recorded. The Civil Disclosure Unit (“CDU”) of North Yorkshire Police will be informed of this decision.

Following review, if no changes are required to this Agreement the CDU will keep a record of the review and new review date will be noted.

If changes are required, the Agreement will be given a new version reference number, the amendments made and it will be reviewed and re-signed by all Partners.

## Audit Arrangements

As part of the requirements of the Code of Practice for the Management of Police Information, the SPOC identified by the Chief Constable for North Yorkshire will maintain an Information Sharing File in respect of this Agreement.

This file which should be electronic will contain:

* A record of North Yorkshire Police information disclosed;
* A record of information disclosed to North Yorkshire Police;
* The decision or justification to disclose or not disclose;
* An access controls and vetting list of Partners;
* Agreed notes of meetings with Partners regarding the information sharing Agreement;
* Details of all relevant correspondence and phone calls; and
* A record of any review of the Agreement.

# POWER OR DUTY TO SHARE INFORMATION

Any information shared and the processes used to share such information will be compliant with the relevant Human Rights legislation and any information will be shared in compliance with the DPA / GDPR as set out in Section 5.

The Crime and Disorder Act 1998 requires relevant authorities to collaborate in the shared aim of reducing crime and disorder. To achieve this purpose, it is necessary to share information about potential/actual perpetrators, victims and survivors of crime.

The sharing of information will therefore be necessary to adhere to this provision.

# LEGAL COMPLIANCE

Adult Victims assessed as Medium to High Risk of harm will be referred by North Yorkshire Police (“NYP”) to PROVIDER so that the above duty to offer the victim/survivor a service can be met. This will be in compliance with:

* Article 6(1)(e) GDPR – public interest
* Article 9(2)(g) GDPR – substantial public interest
* Schedule 1 DPA, conditions 6, 7, 17 and 18 – safeguarding children and vulnerable adults at risk

Lawful basis is ‘Public Task’ - the processing is necessary to ensure the provision of support services to victims of crime under the MoJ Code of Practice for Victims of Crime and safeguarding of children and vulnerable adults.

Adult Victims assessed as Standard Risk of harm, and children or young people will be referred by NYP to PROVIDER after and only when explicit consent is obtained This will be in compliance with:

* Article 6(1)(a) GDPR - consent
* Article 9(2)(a) GDPR – explicit consent

Lawful basis will be ‘Explicit Consent’ - the individual will give clear consent to process their personal data for the specific purpose outlined above and consent to their information being shared between NYP and PROVIDER. If consent is withdrawn, no further information will be recorded, shared or stored.

Individuals will be referred from Supporting Victims Team (“SVT”) acting on behalf of the YNYCA to PROVIDER after and only when explicit consent is obtained. This will be in compliance with:

* Article 6(1)(a) GDPR - consent
* Article 9(2)(a) GDPR – explicit consent

Lawful basis will be ‘Explicit Consent’ - the individual will give clear consent to process their personal data for the specific purpose outlined above and consent to their information being shared between SVT and PROVIDER. If consent is withdrawn, no further information will be recorded, shared or stored.

Neither NYP nor SVT will disclose any other information without explicit consent of the individual, unless there is a risk of harm to the individual or others, or if required by law to share it, in line with Article 6 (1)(c) GDPR.

PROVIDER will then conduct a further, in-depth assessment and deliver the services as required to the individual, reviewing the outcome and result. Once an outcome/result has been achieved, the case will be closed. All referral, assessment, review and exit information will be shared back to SVT acting on behalf of the YNYCA by PROVIDER securely via the YNYCA Case Management System (“CMS”). This will be in compliance with:

* Article 6(1)(a) GDPR - consent
* Article 9(2)(a) GDPR – explicit consent

Lawful basis will be ‘Explicit Consent’ - the individual will give clear consent to process their personal data for the specific purpose outlined above and consent to their information being shared between PROVIDER and SVT. If consent is withdrawn, no further information will be recorded, shared or stored.

In line with the [Code of Practice for Victims of Crime in England & Wales](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974376/victims-code-2020.pdf) the withdrawal of consent at any time will not prohibit an individual from accessing support.

In the course of service delivery, disclosure regarding other crimes, particularly where a sexual or domestic crime is disclosed should be treated appropriately and in line with the PROVIDER’ Safeguarding Policy. In these circumstances and as explained in Section 5.1, it is PROVIDER’ responsibility to ensure individuals understand:

* information may be shared if required to do so by law, in line with Article 6 (1) (c) GDPR;
* any crime(s) reported to PROVIDER, under legal obligation or based on individual permission, may be passed to NYP; and
* NYP have a duty to record and investigate all crimes they are made aware of.

## Duty of Confidence

There are circumstances where a duty of confidence arises and to breach that confidence without reasonable justification could give rise to a complaint and may contravene the DPA / GDPR. This duty of confidence is applicable to all data controllers who are Partners to this Agreement.

Exemptions from this duty of confidence are:

* the individual to whom the information relates has consented to the sharing of the information; or
* the information sharing is required by law.

The following situations do not require consent to share information, but should be addressed on a case-by-case basis to identify why it was not felt appropriate to obtain consent:

* Where there is a statutory duty to share the information;
* When an individual is believed to be at risk of significant harm;
* Where there is evidence of serious public harm, or risk of harm to others;
* Where there is evidence of serious health risk to an individual;
* For the prevention, detection or prosecution of serious crime;
* When instructed to do so by a court; and
* When sharing anonymised or non-person identifiable information.

## Data Protection Act 2018 and General Data Protection Regulations

The Data Protection Act 2018 (“DPA”) and General Data Protection Regulations 2016 (“GDPR”) require that information must be processed fairly and lawfully. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or purposes. Personal data shared under this Agreement will be processed in accordance with the Code of Practice on the Management of Police Information (“MOPI”).

As described above, the exception to this is any crime(s) reported to PROVIDER, under legal obligation or based on individual permission, may be passed to NYP. NYP have a duty to record and investigate all crimes they are made aware of.

Personal data shall not be processed unless one of the conditions in Article 6 of the GDPR is met, and for sensitive/special category data one of the conditions in Article 9 of the GDPR must also be met. Conditions under schedule 1 to the DPA must also be made out where applicable.

This Agreement will, in some circumstances, include the sharing of sensitive and special category personal data.

The following conditions are most likely to be relevant to the sharing of information in circumstances covered by this Agreement. In each case those sharing information should consider that the schedules are satisfied:

Consent:

* GDPR: Article 6(1)(a) – permits processing where the data subject has given consent to the processing of his or her personal data for one more specific purposes;
* GDPR: Article 9(2)(a) – the data subject has given explicit consent to the processing of those personal data for one or more specified purposes; or
* DPA Schedule 1, conditions 17 and 18 – provision of counselling and/or safeguarding children and vulnerable adults at risk.

Services will be provided directly to the individual, in partnership with the parent/legal guardian for children and young people aged 14 years and under, and with parent/legal guardian consent sought. This will not prevent PROVIDER being able to speak directly to children and young people aged 12 - 14 years should they make contact with them directly and in these circumstances, Gillick competency will also be considered as appropriate.

Services will be provided directly to young people aged 14 years and over who are entitled to consent to support themselves, unless there is significant evidence to suggest insufficient capacity following risk assessment of individual circumstances.

When relying on consent, if the data subject is under 14 years old, the processing Partner must obtain parental/ legal guardian consent as appropriate. For children and adults who lack mental capacity to give or withdraw informed consent, this will also be sought from their legal guardian.

Performance of a task in the public interest

* GDPR: Article 6(1)(e) – permits processing where necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
* GDPR: Article 9(2)(g) - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; or
* DPA Schedule 1, conditions 6, 17 and 18 – provision of counselling and/or safeguarding children and vulnerable adults at risk.

## Human Rights Act 1998

Sharing personal and sensitive personal data will interfere with a data subject’s right to a private and family life under the European Convention on Human Rights and Fundamental Freedoms. Any such interference must be in accordance with the law, necessary for the prevention of disorder or crime, public safety or the protection of the rights and freedoms of others.

In each case officers and staff should satisfy themselves that the sharing of information is justified, necessary and proportionate. Information shared should be the minimum necessary to achieve the desired aim.

# TYPES OF INFORMATION TO BE SHARED

This Agreement has been formulated to facilitate the exchange of information between Partners and anonymised summary performance reporting to North Yorkshire Council and the City of York Council as co-commissioners of the services. It is, however, incumbent on all Partners to recognise that any information shared must be justified on the merits of each case. Any information being shared must be proportionate and necessary for the purpose for which it is being shared.

Information will not be shared where disclosure would prejudice ongoing proceedings or sensitive cases unless there is an overriding public safety requirement to do so and in line with Code Of Practice - Criminal Procedure and Investigations Act 1996 and CPS Practice Guidance - Provision of therapy for vulnerable or intimidated adult or child witnesses prior to a criminal trial.

Acting on behalf of the Chief Constable for NYP and the YNYCA, NYP will gain explicit consent to share the following information with PROVIDER:

* Individual personal details (including name, date of birth and ethnicity);
* Individual contact details;
* Crime/incident details;
* Details of referring organisation;
* Brief description of impact of crime(s) or incident(s) and associated support needs of individual;
* NYP officer details;
* Details pertaining to current involved agencies i.e. name of GP or Social Worker and any other special category of personal data freely shared by the data subject that may assist the design and delivery of support to address the abuse experienced e.g. Mental or Physical Health condition;
* Statement of general level of risk (non-specific) from a Public Protection Notice (“PPN”);

No additional information will be shared with PROVIDER unless explicit consent from the data subject has been obtained and documented or required by law to do so as explained above.

Acting on behalf of the Chief Constable for NYP and the YNYCA, SVT will gain explicit consent to share the following information with PROVIDER:

* Individual personal details (including name, date of birth and ethnicity);
* Individual contact details;
* Crime/incident details;
* Details of referring organisation;
* Brief description of impact of crime(s) or incident(s) and associated support needs of individual;
* Details pertaining to current involved agencies i.e. name of GP or Social Worker and any other special category of personal data freely shared by the data subject that may assist the design and delivery of support to address the abuse experienced e.g. Mental or Physical Health condition;
* Details of identified support needs and expectation;
* Statement of general level of risk (non-specific);

No additional information will be shared with PROVIDER unless explicit consent from the data subject has been obtained and documented or required by law to do so as explained above.

Where a referral is made direct to PROVIDER, they will gain explicit consent to collect and share the following information with SVT on behalf of the YNYCA via the CMS:

* Individual personal details (including name, date of birth and protected characteristics);
* Individual contact details;
* Crime/incident details;
* Brief description of impact of crime(s) or incident(s) and associated support needs of individual;
* Details pertaining to current involved agencies i.e. name of GP or Social Worker and any other special category of personal data freely shared by the data subject that may assist the design and delivery of support to address the abuse experienced e.g. Mental or Physical Health condition; and
* Details of identified support needs and expectation or required by law to do so as explained above.

Following receipt of the above information and further assessment of need, the information below will be shared back to SVT on behalf of the via YNYCA the CMS by PROVIDER:

* Completed risk and needs assessment against MOJ nine categories of need;
* Completed cope and recovery plan identifying the individual’s goals and expectations of receiving support;
* Review and exit form upon leaving the service, including a review of the above assessment and plan; and
* Details of any complaints, safeguarding issues and/or disclosure requests (aggregated statistical data) made to PROVIDER by NYP.

Where explicit consent is not given by the data subject, the anonymised/depersonalised information below on an individual level basis will shared back to SVT on behalf of the YNYCA by PROVIDER via the CMS**:**

* Demographic data (including Resident District and protected characteristics);
* Crime/incident details;
* Brief description of impact of crime(s) or incident(s) and associated support needs of individual;
* Details of identified support needs and expectation;
* Completed risk and needs assessment against MOJ nine categories of need;
* Completed cope and recovery plan identifying the individual’s goals and expectations of receiving support;
* Review and exit form upon leaving the service, including a review of the above assessment and plan; and
* Details of any complaints, safeguarding issues and/or disclosure requests (aggregated statistical data) made to PROVIDER by NYP.

The YNYCA will share an anonymised summary performance report on a quarterly basis with North Yorkshire Council and the City of York Council.

The YNYCA will share the share the following anonymised demographic data of those referred by NYP into PROVIDER on a quarterly basis:

* Resident District;
* Age;
* Gender;
* Ethnicity;
* Disability Status;
* Sexual Orientation;
* Pregnancy/Maternity Status;
* Marital Status;
* Religion; and
* Risk Rating.

As explained above at Section 5, at the point of referral onto PROVIDER, the lawful basis will be ‘Consent’ - the individual will give clear consent to process their personal data to support their cope and recovery journey and will consent to their information being shared between NYP or SVT and PROVIDER; PROVIDER back to YNYCA, YNYCA to NYP and PROVIDER to NYP as described above. No additional information will be shared unless explicit consent from the data subject has been obtained and documented, or if there is a risk of harm to the individual or others, or if required by law to share it, this may include in criminal proceedings in line with the Code Of Practice - Criminal Procedure and Investigations Act 1996 and CPS Practice Guidance - Provision of therapy for vulnerable or intimidated adult or child witnesses prior to a criminal trial (<https://www.cps.gov.uk/publications/prosecution/pretrialadult.html>

and <https://www.cps.gov.uk/publications/prosecution/therapychild.html>).

If consent is withdrawn, no further information will be recorded, shared or stored.

NYP may only request information from PROVIDER using the attached disclosure request form, quoting the legal gateway.

When making the decision whether to disclose to NYP, PROVIDER must consider the information requested to meet the legal gateway quoted and document the rationale as to why or why not information has been disclosed.

If the information requested is disclosed, only the information that serves the purpose will be shared, not the whole file.

The number of disclosure requests (aggregated statistical data) made to PROVIDER by NYP will also be recorded during Contract Performance / Management meetings with the YNYCA Commissioning and Partnerships Manager. No identifiable or sensitive information will be disclosed in the meeting.

# ROLES AND RESPONSIBILITIES

Each Partner, and North Yorkshire Council and the City of York as a co-commissioners of the services will appoint a Single Point of Contact (“SPOC”) who will be a manager of sufficient standing and understanding and who will have a co-ordinating and authorising role. A Partner may also appoint a supervisor or manager to deputise for the SPOC.

The following named individuals are the SPOCs and Deputies for the Partners and North Yorkshire Council and the City of York as a co-commissioners of the services who will be responsible for data protection, security and confidentiality, and compliance with all relevant legislation:

|  |  |  |  |
| --- | --- | --- | --- |
| **NAME** | **POST** | **ORGANISATION** | **CONTACT DETAILS** |
| **TBC** | **TBC** | **North Yorkshire Police** | **TBC** |
| **Sally Lynch** | **Commissioning and Partnership Manager** | **Policing, Fire and Crime Directorate, York and North Yorkshire Combined Authority** | **Email:**  **Tel:** |
| **TBC** | **TBC** | **(PROVIDER)** | **TBC** |
| **TBC** | **TBC** | **North Yorkshire Council** | **TBC** |
| **TBC** | **TBC** | **City of York Council** | **TBC** |

The specific responsibilities of the above SPOCs and deputies are:

* Making sure the named Partner abides by this Agreement;
* Ensuring relevant staff are fully aware of their responsibilities;
* Appointing other staff to act in their absence;
* Controlling the release of the information and maintaining its integrity;
* Deciding on a case-by-case basis for more complex cases, if necessary, if and why a public interest overrides a duty of confidence;
* Keeping an information sharing file which holds all the Partner’s information sharing documents in general; and
* Ensuring any changes to the SPOCs details are confirmed in writing.

# PROCESS OF SHARING

The information may only be used for the purpose/s set out in this Agreement.

Partners to this Agreement will respond to any notice from the Information Commissioner that imposes requirements to change the way in which personal data is processed or to cease processing personal data.

## Access to the Information

The information may only be used by the Partners to contact, support and inform the risk assessment when working with those directly affected by domestic abuse.

The information will be shared securely via secure email, stored in a secure place and kept in accordance with the DPA and the terms of this Agreement including the Force Information Security Policy, Protective Marking Procedure and the Security Aspects Letter as per contractual agreements.

Only personnel within the receiving Partner organisation that have a lawful requirement to access the information in connection with the purposes for which it is shared, will have such access.

## Sharing Procedure

Acting on behalf of Chief Constable for NYP and the YNYCA, NYP will process data from the NYP’s record management system, NICHE to inform/update PNNs to share information as indicated in section 6 with PROVIDER via secure email.

Acting on behalf of the YNYCA, SVT will share information as indicated in section 6 with PROVIDER through the YNYCA’s CMS.

PROVIDERwill share information as indicated in section 6 with SVT through the YNYCA’s CMS and with the YNYCA at Contract & Performance Monitoring meetings.

## Ensuring the Accuracy of Information Shared

Version:1.10.0.3

Hash:/cH4U9xyFu5funa4qUJW3AjdZ1c=

Information discovered to be inaccurate or inadequate for the purpose will be notified to the data owner who will be responsible for correcting the data and notifying all other recipients of the data who must ensure that the correction is made.

Partners are responsible for ensuring that any information they share is accurate and, where necessary, kept up to date.

## Information Management

Partners to this Agreement undertake that personal information shared will only be used for the specific purpose for which it is requested. The recipient of the information is required to keep it securely stored.

Review, Retention & Disposal

Data will be subject to annual review and when no longer required for legitimate purpose as per this Agreement will be disposed of in accordance with Government Security Classification marking requirements.

This shared data will be reviewed, retained and disposed of in line with both the Chief Constable of NYP and the YNYCA’s Retention Schedules.

Hard copy information will be disposed of confidentially through the use of shredding machines, and electronic data will be deleted.

The SPOCs identified in this Agreement will be responsible for ensuring this takes place.

## Information Security

The information must be stored securely at all times and destroyed when it is no longer required for the purpose for which it is provided.

The information shared must not be disclosed to any third party without the written consent of the Partner that provided the information; unless it is disclosed under a statutory obligation or by NYP for a policing purpose.

### Information Security Governance & Risk Management

It is expected that Partners to this Agreement will have in place baseline security measures compliant with BS17799:2005 and International Organisation for Standardisation (ISO) / IEC 27001:2005, and HMG standards in relation to information security. Only nominated representatives can access, request information, and make disclosure decisions. Data must be stored securely to prevent unauthorised access and disclosure.

The Partners to this Agreement will continue to apply those relevant security obligations for the length of this Agreement. Each Partner agrees to apply appropriate security measures, commensurate with the requirements Article 5(1)(f) GDPR: to ensure all relevant data is ‘processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or dame, using appropriate technical or organisational measures’.

The Partners will ensure that first line supervision / management periodically review / audit the data shared or work carried out to ensure it is within the scope of this Agreement and purpose.

The Partners will enforce their respective organisational policies to govern the appropriate behaviour and instil good security working practices within their organisation including clear screen / desk, password management, information security & file classification.

### Access Control

The Partners will ensure that restricted access and control mechanisms are in place to limited who has access to the shared information. Such staff who have an operational need to access, view, store & analyse these data sets or to provide direct support and maintenance will be governed under the need to know principle & they will have a allocated task directly related / relevant to the shared information. All relevant data will be saved in appropriately secure locations with limits to who can access / view / write to the data sets.

Audit trail of all activity in the processing of shared data will be available. This will include all interactions and modifications with the information and the associated documents to enable identification of:

* Request type / sharing platform (in meeting or independent request) including date and time;
* Access (by user ID);
* Updates (date and time); and
* Decisions (what was accessed, created and/or modified /deleted.

### Security Architecture & Design

The Partners will ensure that they commit to protecting the shared information by employing physical, technical and administrative processes to safeguard and secure the data. Ensuring that traffic monitoring, maintenance & configuration is suitably managed. For example, Information will be securely stored by the Partners on password protected computers and locked away in secure cabinets when not in use. Any security incidents will be immediately escalated to the Data Protection Officers for both NYP and the YNYCA.

The information will be:

* Held in a secure location that meets the requirements of the Partners governance and information security policies;
* Held in a secure location that meets the requirements of North Yorkshire Police and the National Cyber Security Centre’s guidance; and
* Able to securely store data of the protective mark Official Sensitive.

The Partners will ensure that the information is processed / stored in a segmented manner from other data sets.

### Physical & Environmental Security

The Partners will ensure that they commit to protecting the shared information by employing physical security measures suitable to prevent (not an exhaustive list) unauthorised access, disclosure, theft, dumpster diving

Any Partner visits to NYP will be by appointment only and visitors will be escorted and managed whilst on site at all times in line with the Information Security Policy.

### Telecommunications & Network Security - nil

### Cryptography – nil

### Business Continuity & Disaster Recovery

The Partners will within reasonable time provide notice of any maintenance requirement, system failures or resilience issues which may impact the service delivery of NYP.

### Legal, Regulations, Compliance & Investigations

Where NYP/YNYCA information resides with a Partner, there is the possibility that breaches of security will occur.

Should a breach in security occur in relation to information of the Chief Constable for NYP or the YNYCA, the Partner(s) should within 24hrs submit a Data Breach Reporting Form (Annex A) via email to the YNYCA’s SPOC in the first instance who will submit a Security Incident Report to notify the Information Security Officer and Data Protection Officers for both the Chief Constable for NYP and YNYCA.

The Partners will work in collaboration to reduce the risk to any NYP/YNYCA data prior to, during and post any security incident.

It is also important to note that such incidents will be recorded and reported upon, and where it is discovered that any partnership is posing a threat to NYP through repeated incident occurrences, the continuance of such partnerships will be reviewed.  Partners will be advised of the outcome of any evaluation.

### Software Development Security – nil

### Security Operations

The Agreement can be used to apply a protective marking to the information being shared in line with the Chief Constable for NYP’s Governmental Security Classification Procedure, where applicable. Where NYP shares information with others who do not recognise Protective Marking, the decision as to who has access and what they may use it for, is a risk-based decision.

If there is any cause for any ‘official’ or above NYP information to be transferred between the Partners the information will be appropriately marked with a file classification & handling condition. Any data transferred must be appropriately protectively marked with the recipient been made aware of such labelling / handling conditions.

The author employed by either Partner will ensure that any document created and marked with the appropriate file classification, they will consider the duration of the classification or review period.

If there is any cause for any ‘official’ or above NYP information to be transferred between the Partners must be encrypted whilst in its form of transmission sent via the Police National Network (PNN) email. If either Partner has alternative secure communication transferring portals, it may be used by NYP upon the authority of the Information Security Officer.

If there is any cause for any ‘official’ or above NYP information to be transferred between the Partners which are too large to share via the PNN network via encrypted email. Large datasets can be sent via storage medium but the file must be encrypted on a storage medium & despatched to the recipient via a procured courier service using a special delivery ‘signed for with tracking’ service or similar. Encryption password will be communicated as a separate form of communication i.e. via email ensuring that both the storage medium & password are NOT sent together.

If either Partner has alternative secure communication transferring portals, it may be used by NYP upon the authority of the Information Security Officer.

Any data transferred between systems shall be transferred securely and in line with NYP’s Information Security policies.

If there is any cause for either Partner to print out shared information, it must be retrieved by the associated members of staff who have a need to know, view, access, store and process these data sets.

If there is any cause for either Partner to print out shared information, it must be securely dispose of using cross cutting shredder and disposed of in confidential waste bins.

*The Information Security Officer from NYP will, by arrangement, undertake a review of the security in place to ensure the confidentiality, integrity, availability and non-repudiation of the Partners’ information being stored under this Agreement.*

# MISCELLANEOUS MATTERS

## Indemnity

Partners to this Agreement are aware that the deliberate or reckless disclosure of personal data (obtained under this Agreement) to other organisations or persons may amount to an offence under Section 170 of the DPA.

Partners to this Agreement indemnify the Chief Constable of NYP (to include the Chief Constable, officers and staff, and the YNYCA and staff) against any costs, damages and expenses it incurs in connection with and arising from legal claims (of whatever nature) against NYP arising from this Agreement, to include, but not limited to, claims arising from an alleged breach of this Agreement, misuse of the information or wrongful disclosure by the Partner and breach of confidentiality, save where the claim arises directly and solely because of the negligence of NYP.

## Access Rights of Data Subjects

If a Partner to this Agreement receives a subject access application under Section 45 of the DPA or Article 15 of GDPR and personal data is identified as belonging to another Partner or a third party to this Agreement, it will be the responsibility of the receiving Partner to contact the data owner to determine whether the latter wishes to rely on the right to any statutory exemption under the provisions of the DPA. Where the information cannot be provided without disclosing information relating to another individual who can be identified from that information, there is no obligation to comply with the request unless the other individual has consented to the disclosure of the information to the person making the request, or it is reasonable in all the circumstances to comply with the request without the consent of the other individual. In determining whether it is reasonable, regard shall be had, in particular, to:

1. any duty of confidentiality owed to the other individual;
2. any steps taken by the data controller with a view to seeking the consent of the other individual;
3. whether the other individual is capable of giving meaningful consent; and
4. any express refusal of consent by the other individual.

## Freedom of Information Act Considerations

If a Partner receives a request for information under the Freedom of Information Act 2000 and the information requested is identified as belonging to another Partner or third party to this Agreement, it will be the responsibility of the receiving Partner to contact the data owner to determine whether the latter wishes to rely on any statutory exemption under the provisions of the Freedom of Information Act and to identify any perceived harm.

# SIGNATURES

By signing this Agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purpose of this Agreement.

Signatories must also ensure that they comply with all relevant legislation.

DRAFT EXAMPLE PROVIDED FOR INFORMATION ONLY – DO NOT SIGN THIS VERSION

**Appendices**

**Annex A – Data Breach Reporting Form**

