North Notts Business Crime Reduction Partnership (NNBCRP)

Data Privacy Impact Assessment

February 2021

Contents

1. Purpose of this Data Privacy Impact Assessment

1.1 North Notts Business Crime Reduction Partnership (**NNBCRP**) is a not for profit public private partnership for intelligence collaboration supported by both business and the law enforcement community to help tackle the growing threat of business crime whilst minimising the demand on policing. It has the support from the Nottinghamshire Police and Crime Commissioner. It is working closely with Bassetlaw District Council, Retford & Worksop Business Forums, Retford & Worksop Civic Societies. The **NNBCRP** also continues to forge relationships with a range of other law enforcement partners such as Worksop & Retford Shopwatch, Worksop & Retford Pubwatch and the Dukeries Rural Watch Group.

1.2 The **NNBCRP** brings together a number of businesses that in isolation are having a minimal effect on crime reduction, but in collaboration are capable of pooling sufficient resource and information to have a significant effect on crime reduction within their member's geographical locations.

1.3 The purpose of the **NNBCRP** data privacy impact assessment (DPIA) is to mitigate or minimise risks to data subjects and minimise business risks to the **NNBCRP**, its stakeholders and its business members. The DPIA must:

a) Describe the nature, scope, context and purposes of the processing;
b) assess necessity, proportionality and compliance measures;
c) identify and assess risks to individuals; and
d) identify any additional measures to mitigate those risks.

2. Explanation of flows of personal data within NNBCRP

Please see DPIA data flows –

1) **NNBCRP** information flow bulk data – Getting business crime incident data into the **NNBCRP**

This flow demonstrates data transfer processes from **NNBCRP** business members providing such data to the **NNBCRP** crime management software and appropriate **NNBCRP** deletion protocols.

2) **NNBCRP** information flow intelligence – Getting specific intelligence data into the **NNBCRP**

This flow demonstrates data transfer processes from **NNBCRP** business members providing specific intelligence data to the **NNBCRP** crime management software and **NNBCRP** appropriate deletion protocols.

3) **NNBCRP** information flow service delivery – How the **NNBCRP** handles data

This flow demonstrates how the **NNBCRP** will handle, conduct analysis and transfer relevant proportionate business crime data alerts to business members, Policing / Law enforcement bodies via secure system transfer, or secure email only with the purpose of the prevention and detection of crime and supporting preventative business risk activity. This includes the **NNBCRP** crime management software member access, the appropriate deletion protocols are covered in earlier data flows.

4) Data subject access request – How the **NNBCRP** handles subject requests

This flow demonstrates how the **NNBCRP** handles subject data access requests and appropriate responses dependant on whether the data subject is currently subject to an ongoing criminal investigation.

3. NNBCRP processing scope and types of data shared

3.1 The **NNBCRP** will act as the data controller and any processing is conducted under information sharing agreements with UK law enforcement bodies, its business members, UK crime partnerships and any other relevant bodies or businesses linked to ongoing criminal investigations, or for the purpose of analysing such data to further investigations into cross company, cross Police force prolific persistent offenders (PPO) – This is commonly known as receiving level 1 crime information identifying level 2, or level 3 offenders, as described in the Policing National Intelligence Model (NIM) methodology. The processing will include special category and criminal offence data due to its nature.

Information sharing with **NNBCRP** *Members*

3.2 The **NNBCRP** receives and shares business crime data from member businesses with a view to enabling businesses to take preventative action, or make consumer decisions regarding data subjects, the **NNBCRP** will not make denial of service decisions, the **NNBCRP** member will make these of their own accord.

3.3 The data will be collected from multiple Businesses meaning the amount of data collected and processes will be sizeable. There are strict deletion protocols in place with a 12-month deletion rule for data which becomes irrelevant. The nature of the service means the data coverage will be in and around the Bassetlaw area, no data will be processed or stored where the source is from outside of these counties unless it is provided to **NNBCRP** by third party and meets the purpose of the data processing. Multiple individuals concerned with criminality will be affected by the data processing.

3.4 The business crime data received from members can include any of the following:

- Photographs/CCTV
- Vehicle registration information
- Names addresses
- Modus operandi of known or suspected criminals
- Dates of Birth
- Physical descriptions
- Unique identifiers

Information sharing with law enforcement bodies, including the Police

3.5 Information sharing agreements with law enforcement authorities provide a mechanism for such authorities and **NNBCRP** to share certain personal and criminal conviction and offence data, as well as detailed crime statistics, as appropriate, in respect of persons convicted or suspected of involvement in business related crime. This information will comprise of:

- extracts of data from police intelligence crime recording and custody imaging systems
- conviction information and also non-conviction information in respect of arrests, charges and cautions
- Other non-conviction information and images may be shared to achieve the purpose on a case by case basis if it is deemed to be proportionate, lawful and necessary.

This information will only be shared with **NNBCRP** Members and other partners where the data sharing meets the agreed purpose of the data processing.

3.6 Information sharing agreements with law enforcement bodies allow such bodies to publicise to **NNBCRP** any offenders who are likely to be cross company, or cross force persistent, prolific offenders, or who have received an Order under relevant Anti-Social Behaviour legislation which prohibits them from entering any part of the area, or member premises. **NNBCRP** members will be able to assist the police in identifying persons in breach of these Orders. Such information circulated to specific partners may consist of individual or a mix of the following special category data.

4. Context of NNBCRP Data Processing

4.1 **NNBCRP** processing activity includes the following processing a) Large scale uses of sensitive data; b) Data matching from multiple sources (E.G. VRM, MO, Images, postcode, email, telephone number or carriers); & c) The possible targeting of children or vulnerable persons. Any data received by the **NNBCRP** is provided by its members on the understanding that the data subjects concerned have been, or are likely to have been involved in crime against that member.

4.2 The **NNBCRP** will have no relationship with the data subjects, the **NNBCRP** acts as an agent of its Members to identify patterns in criminal behaviour and work with various and appropriate law enforcement bodies to identify the true extent of the criminal behaviour in order to effect appropriate Police / agency action or business preventive action to prevent further offending. The data subjects will have no control over their data and the **NNBCRP** expects the subjects would be unaware of our involvement with their data as their interaction is with the **NNBCRP** Member business who have their own DPIA supporting their own processing activities.

5. Purpose of NNBCRP Data Processing

5.1 The aim of the **NNBCRP** is to support member businesses, the Police and other agencies in the reduction of Business Crime through partnership work, intelligence sharing and target hardening support. The intended effect on the data subjects is enabling appropriate action commensurate to the data subject's activities supporting appropriate prevention and detection in order to disrupt further criminal behaviours. The **NNBCRP** does not deny service to data subjects but provides intelligence to support individual decision processes. The **NNBCRP** benefits from this type of processing through increased credibility and increased membership, this in turn allows the **NNBCRP** to develop new products and services and further support the business community.

5.2 The **NNBCRP** brings together a number of businesses that in isolation are having a minimal effect on crime reduction, but in collaboration are capable of pooling sufficient resource and information to have a significant effect on crime reduction within their member's geographical locations.

Benefits to Police and law enforcement bodies

5.3 The **NNBCRP** collaboration supports such partnerships as recommended in the Crime and Disorder Act 1998, which places a responsibility on Police to work in partnership with other agencies, organisations and individuals in the furtherance of the reduction of crime and anti-social behaviour and the reduction of the fear of crime and anti-social behaviour in the community.

5.4 Benefits to the Police will include the reduction of crime and anti-social behaviour for members of the **NNBCRP**; improved opportunities for the apprehension of offenders; and reduction in the fear of crime. This will be measured in crime statistics and outcomes obtained from crime reporting systems and qualitative feedback from the community provided in member service level agreement meetings.

5.5 This information sharing process will increase opportunity for better partnership working within the business community. It will also assist the local Crime Reduction strategy. Statistically, levels of detections in areas participating in a crime reduction scheme improve, on a national level, from 26% to 82% (Action Against Business Crime AABC 2008). The primary reason for this is the improved intelligence from the sharing of information.

Benefits to **NNBCRP** *members*

5.6 The furtherance of BCRP/BID partnership working helps to focus partnership awareness of local crime and improve the quality of shared intelligence with police and other agencies. All businesses will benefit from the reduction of crime and anti-social behaviour within the business district. This in turn encourages better co-ordination of police and partnership resources to deter and prevent crime.

5.7 Sharing relevant information improves the safety of employees within the area. It also assists in protecting the assets of the businesses trading within the area. The increased levels of detection will improve profitability and maintain a healthy consumer market, which is currently maintained by a combination of residents, commuters and tourists. Protecting these sections of the community improves the sustainability and continuity of the local business partners.

5.8 In addition, members will be alerted to the fact that habitual troublemakers who may already be subject to their exclusion schemes, or other interventions may also be subject to orders or restrictions imposed under relevant ASB legislation and thus will identify occasions when police may be best suited to deal with certain issues rather than placing employees at risk.

5.9 Specific examples to **NNBCRP** members of results achieved through data sharing with **NNBCRP** are set out below:

- **NNBCRP** is able to collate and link offence data provided by individual **NNBCRP** Members; this means offence data can be collated and provided to the Police as series linked investigations, making it more likely that offender will be apprehended through Police action. Such reporting makes eventual apprehension much more likely than individual reporting of crimes to the Policy by **NNBCRP** members.
- Members are more likely to report known or suspected offenders to **NNBCRP** than to the Police; **NNBCRP** is able use such offence data provided by Members to identify and analyse trends and generate reports; this in turn helps the Police and the member develop better strategies for dealing with crime.
- **NNBCRP** can identify prolific and persistent offenders targeting multiple businesses and personally serve exclusion notices against these individuals removing their implied right to enter those businesses; this in turn reduces the likelihood that those individuals will re-enter those business premises and commit further crime. Additionally, should that individual breach the exclusion notices then the **NNBCRP** can support that Member Business with Civil Court Injunction. This action further prevents the individual entering the member premises and if breached can constitute contempt of court.

Benefits to the Community

5.10 Local communities will benefit from being able to enjoy safer environments in which to shop, live, work and commute. This may also encourage more shoppers to the areas and thereby stimulate local economic growth. Some businesses may be encouraged to invest some profits back into community ventures through sponsorship or other funding. In addition, there may be an increase in the number of special offers and promotional sale events. An increase in customers could create more employment opportunities and increased area affluence can have a positive impact on local property prices.

6. NNBCRP Consultation Process

6.1 Privacy impact consultation and review will be a formal part of the quarterly NNB Board meetings. The Board meetings minutes will reflect any need to amend any processes.

6.2 We have engaged with external Information Security Practitioners for advice and guidance and will maintain this relationship for the foreseeable future.

6.3 Members will be reminded of the data requirements during Service Level Agreement meetings and **NNBCRP** will work in partnership with its members to ensure compliance to minimum standards covering both the **NNBCRP** DPIA and the member DPIA, this includes the control measures applied to identified risks for both parties both during service delivery and product onboarding.

7. Compliance with the Data Protection Principles and Legal Basis for sharing personal data, special category data and criminal offence data

Legal background

7.1 Data Protection Law acts as a framework for how to process (including share) personal, special category and criminal offence data. The Data Protection Act 2018 (**DPA**) incorporates the EU General Data Protection Legislation ((EU) 2016/679) (**the GDPR**) into UK law. The GDPR prohibits personal data processing unless there is a lawful basis for that processing as set out in Article 6. Further provisions relate to **special category data** and **criminal conviction/offence data**, as set out below.

Special category data

7.2 Processing of special category data including data revealing racial or ethnic origins is prohibited under Article 9(1) of the GDPR unless one of the conditions in Article 9 (2) applies. In order to lawfully process special category data, it is necessary to identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9(2) of the GDPR. Schedules 1 and 2 of the DPA contain specific conditions and safeguards applicable to each of the grounds in Article 9(2).

Criminal conviction/ offence data / “competent authorities”

7.3 In order to process such data, it is necessary to identify both a lawful basis under Article 6 and also necessary to comply with Article 10 GDPR. Article 10 states that such data can only be processed “under the control or official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. **Any comprehensive register of criminal convictions shall be kept only under the control of official authority.**”

7.4 A competent authority is:

(a) a person specified or described in Schedule 7 of the DPA, and
(b) any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.

7.5 The Law Enforcement Directive 2016/680 has been implemented into UK by Part 3 of the Data Protection Act 2018. This regulates the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The processing of criminal conviction data which is not carried out under the control of official authority must meet one of the conditions in Parts 1, 2 or 3 of Schedule 1 of the DPA.

7.6 **NNBCRP** is not a competent authority and therefore, under section 10(5) of the DPA, its processing of criminal conviction/offence data must meet one of the conditions in Parts 1, 2 or 3 of Schedule 1 of the DPA.

7.7 The police and other law enforcement bodies with who **NNBCRP** share data may be competent authorities under schedule 7 of the DPA 2018. If so, the processing of criminal offence data by such bodies will be regulated by Part 3 of the DPA and is dealt with in the information sharing agreements between **NNBCRP** and such bodies, including the Police.

NNBCRP *does not hold a "comprehensive register of criminal convictions"*

7.8 Article 10 of the GDPR states that "any comprehensive register of criminal convictions shall only be kept under the control of official authority". Whilst **NNBCRP** receives criminal conviction data, it does not maintain a comprehensive register of criminal convictions in the sense that that register is not a complete register of convictions. If **NNBCRP** receives criminal conviction data about data subjects, this is recorded in "note form" in the database. However, the receipt of such data is "sporadic" and no "comprehensive" or complete register is maintained.

First Principle

Data must be processed lawfully, fairly and in a transparent manner in relation to the data subject

7.9 **NNBCRP** achieves this principle by:

- Working with an appropriately resourced Data Protection representative, who is responsible for maintaining data protection across the organisation and is empowered to challenge how personal data is used.
- Maintaining privacy notes that clearly state what personal data it collects, who the data controller is, who **NNBCRP** shares personal data with, why **NNBCRP** collects personal data, how personal data will be used, who **NNBCRP** shares it with, the legal basis for processing the personal data, how long **NNBCRP** will hold the personal data for, how to contact the Data Controller, the right to object to processing and how to contact the ICO in event of a complaint.
- Maintaining a subject access request procedure and associated register to demonstrate that **NNBCRP** is responding to requests within 30 days.
- Conducting data protection impact assessments on all new projects that may directly impact the privacy of data subjects, led by the **NNBCRP** supported by the Data Protection representative.
- Maintaining records of processing activities, so that **NNBCRP** can demonstrate a full understanding of its use of personal data.
- Maintaining **NNBCRP** registration with the ICO.

Lawful Basis for Sharing Personal Data

7.10 The processing of personal data must satisfy at least one condition in Article 6 of the GDPR in relation to personal data.

7.11 Article 6(f) of the GDPR states that the processing is lawful if the:

> “processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

7.12 Guidance from the Information Commissioner’s office on Article 6(f) states that there are three elements to the legitimate interest test. A controller needs to:

- Identify a legitimate interest;
- Show that the processing is necessary to achieve it; and
- Balance it against the individual's interests, rights and freedoms.

7.13 The legitimate interests:

- Can be the controller's or those of third parties.
- Can include commercial interests, individual interests or broader social interests.

7.14 The legitimate interest being pursued by **NNBCRP** is to run successful businesses in a safe environment for both staff and customers and there is no other reasonable means of achieving this. The sharing of information will not override the rights and freedoms of the data subjects and will not cause any unjustified harm.

7.15 **NNBCRP** only uses data subject information of those who have been or are highly likely to have been involved in criminal acts against member businesses, this may include juveniles, children or vulnerable person data and other special category data as they may have been involved in the commission of these acts.

7.16 The **NNBCRP** understands its responsibilities and is confident that this legitimate interest data use is the most appropriate and lawful way of sharing appropriate data to prevent, detect and deter criminality.

7.17 The data processing overrides the rights and freedoms of the data subject as the subject has been or is suspected of being involved in criminal activity. The data sharing is minimal and is critical to the prevention and detection of criminal acts.

7.18 The role of **NNBCRP** is the effective prevention and detection of crime and the significant outcomes it is able to achieve in assisting the Police and other law enforcement bodies is set out in paragraph 5.9 above.

Lawful Basis for Sharing Criminal Offence Data

7.19 **NNBCRP** is not a competent authority and therefore its processing of criminal conviction/offence data must meet one of the conditions in Parts 1, 2 or 3 of Schedule 1 of the DPA (Section 10(5) DPA).

7.20 Schedule 1 Part 2 of the DPA includes substantial public interest conditions for sharing data including when the processing of such offence data is “**necessary** for the purposes of the prevention or detection of an unlawful act, must be carried out without the consent of the data subject so as not to prejudice those purposes and is necessary for reasons of substantial public interest” (paragraph 10, *Preventing or detecting unlawful acts*). As long as the processing is “necessary” for the purpose , consent of the data subject is not required if this would be prejudice the prevention or detection of the unlawful act. DPA 2018, Sch 1, Pt 3 provides that processing of criminal offence data is permitted if the processing would meet a condition in DPA 2018 Sch 1, Pt 2, but for an express requirement for the processing to be necessary for reasons of substantial public interest. This means that that the substantial public interest element of the condition is not necessary in relation to criminal offence data.

7.21 The explanatory notes to the DPA state that this condition 'permits processing of special categories of data for the purposes of the prevention or detection of any unlawful act where it is necessary for reasons of substantial public interest (although this substantial public interest element does not apply in relation to criminal offence data) or where seeking the consent of the data subject to the processing would prejudice those purposes, which would cover a situation where giving the data subject a choice or giving them the necessary information required for valid consent would prejudice the purpose, or where valid consent is not possible because a refusal to consent could cause detriment.'

7.22 **NNBCRP** processing of criminal offence data is reviewed on a case by case basis and the data sharing is minimal and is critical to the prevention and detection of criminal acts. Guidance from the ICO on the meaning of "necessary" states this does not mean that processing always has to be essential, but it must be a targeted and proportionate way of achieving the purpose. **NNBCRP** processes criminal conviction data in a targeted and proportionate way in order to prevent and detect unlawful acts. The significant and proven contribution of **NNBCRP** to crime detection and prevention is set out in paragraph 5.9 above. Relevant information related to crime and the prevention of crime, held by **NNBCRP**, for such purposes as implementation of individual exclusion processes, the execution of proactive industry operations and other operations with the intention of lowering business-related crimes will only be passed to the Police if there is a belief that the information is not already in possession and is in the public interests of safety and social economic wellbeing. *Sharing information supports the prevention and detection of crime in several ways;* 1) Assists in the identification of offenders 2) Enables the true scale of the issues to be demonstrated to Members and Policing 3) Enables effective reporting of the true scale of business crime into the Home Office to enable appropriate policy making.

7.23 The sharing is "necessary" for the prevention and detection of crime because **NNBCRP** could not reasonably achieve its purpose by any other means.

Appropriate Policy Document

7.24 When **NNBCRP** is disclosing criminal offence data to a competent authority then there is no need to have an appropriate policy document in place but, as required under Article 30 of the GDPR, a record is maintained by **NNBCRP** which identifies the processing condition that is being relied on under the DPA (the prevention or detection of unlawful acts) and which lawful basis is being relied upon under Article 6 GDPR (legitimate interest).

7.25 For all other processing of criminal offence data other than disclosure to a competent authority, **NNBCRP** has an appropriate policy document in place which:

(a) explains **NNBCRP**'s procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the relevant condition (the prevention or detection of unlawful acts), and

(b) explains **NNBCRP** policies as regards the retention and erasure of personal data processed in reliance on the above condition, giving an indication of how long such personal data is likely to be retained.

This will made available to the ICO on request.

7.26 If the disclosure is made under this provision **NNBCRP** is exempt from providing the information required by Articles 13 and 14 of the GDPR to the data subject to the extent that this would prejudice the purposes of preventing or detecting unlawful acts or for the apprehension or prosecution of offenders.

Lawful basis for sharing special category data

7.27 If the information is "sensitive" as defined in section 35(8) of the DPA or "special category" as defined in Article 9 GDPR (that is, where it reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trades union, physical/mental health, or sexual orientation or sex life) then processing is only permitted in certain cases.

7.28 The processing of special category data is prohibited under the GDPR unless one of the conditions set out in Article 9(2) applies and in relation to the **NNBCRP** subparagraph (g) allows:

> *"processing [which] 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 protection and provide for suitable and specific measures to safeguard the fundamental data rights and the interests of the data subject".*

7.29 The relevant Member State Law is the DPA, where section 10(3) states that processing meets the requirements in Article 9(2)(g) of the GDPR only it meets a condition in Schedule 1, Part 2 of the DPA. The ground relied on here is the same as that set out in paragraphs 7.19 and 7.20 above in relation to criminal offence data and the substantial public interest condition is relevant. The ways in which **NNBCRP** sharing of data is in the public interest is set out in section 5 above.

7.30 When **NNBCRP** is disclosing special category data to a competent authority then there is no need to have an appropriate policy document in place but, as required under Article 30 of the GDPR, a record is maintained by **NNBCRP** which identifies the processing condition that is being relied on under the DPA (the prevention or detection of unlawful acts) and which lawful basis is being relied upon under Article 6 GDPR (legitimate interest).

7.31 For all other processing of special category data other than disclosure to a competent authority, **NNBCRP** has an appropriate policy document in place which:

(a) explains **NNBCRP**'s procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the relevant condition (the prevention or detection of unlawful acts), and

(b) explains **NNBCRP's** policies as regards the retention and erasure of personal data processed in reliance on the above condition, giving an indication of how long such personal data is likely to be retained.

Second Principle

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

7.32 The information shared by **NNBCRP** will be that which was originally obtained for the prevention / detection of crime and / or the apprehension / prosecution of offenders.

7.33 Sharing this information with a third party, in this case **NNBCRP** members or the Police or other law enforcement bodies, will not result in the information being processed in any manner contradictory to the original purpose.

7.34 If **NNBCRP** is disclosing personal data to Police using the legal basis set out in Part 1 of Schedule 2 of the DPA, where it has decided that not sharing the personal data would prejudice the prevention and detection of crime or the apprehension or prosecution of offenders, then National Business Crime Solution (**NNBCRP**) does not need to comply with the second principle to the extent that it would prejudice the purpose of the sharing.

Third Principle

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7.35 **NNBCRP** achieves this principle by:

- minimising the personal data it holds and processes;
- de-identifying the data, whenever business processes allows;
- formally reviewing the adequacy and relevant of personal data annually, adjusting where it finds that personal data is not relevant or is not adequate and this is captured in the data asset register;
- only sharing data with organisations to whom it is relevant and ensuring that the minimal amount of data should be share for the purposes set out in this DPIA.

Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

7.36 **NNBCRP** achieves this principle by:

- Maintaining processes that assure the quality of personal data shared with **NNBCRP**, advising the source when **NNBCRP** finds that data to be inaccurate or of poor quality;
- Maintaining processes that keep personal data up to date.
- Making it easy for data subjects to ask for their personal data to be rectified or erased, when legally permissible.
- Erasing or rectify data that is found to be inaccurate or out of date with 72 hours of discovery.

Fifth Principle

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

7.37 **NNBCRP** achieves this principle by:

- Maintaining a 12 month records retention schedule, that aligns with established best practice and law.
- Reviewing its use of personal data and destroy information when it no longer supports the define purpose for processing it.

Sixth Principle

Personal data shall be 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 damage, using appropriate technical or organisational measures.

7.38 **NNBCRP** achieves this principle by:

- Establishing an effective information security policy framework, which aligns with ISO27001.
- Designing processes with 'privacy by design' in mind.
- Maintaining procedures that:

a) Identify assets, which impact personal data.
b) Map data flows of personal data.
c) Risk assess assets and data flows.
d) Identify owners of assets, risks and data.
e) Control the disposal of personal data.
f) Manage the transfer and sharing of personal data.
g) Seek assurance from our third-party partners.
h) Put in place information sharing agreements, so that we all have a common understanding of the use and protection of personal data.

i) Manage information security incidents, learning from them to prevent reoccurrence and reporting to the ICO when required.

j) Establish clear roles and responsibilities for all staff, so that they understand what is expected of them and who to contact for support.

k) Effectively manage joiners, movers and leavers within the organisation.

l) Provide our staff with training and supervision, so that they can confidently handle personal information and systems that process it.

8. What information will we give Individuals?

The **NNBCRP** will have a privacy statement on our website informing the public of our activity and business purpose.

9. Internal Conformance and review

9.1 The **NNBCRP** will have the following safeguards in place to ensure compliance to process;

1. Internal policies
2. Governance and Management – PIA, technical controls and business controls
3. Documented training and awareness including
    a. Training and awareness
    b. Data accountability
    c. Access control
    d. Data destruction
    e. Incident management
4. Third party Management
    a. Due diligence
    b. Contracts
    c. Information Sharing Agreements
5. Regulatory Advice
    a. Regulation requirements
    b. Minimising data collection and use
    c. International Transfer Control
6. Data Subject Rights
    a. Regulatory Requests
    b. SARS
    c. Deletion Protocols
    d. Investigations
7. Retention
    a. Retention
    b. Archiving
    c. Destruction
        i. Systemic controls

Process of regular review
The **NNBCRP** conducts quarterly **NNBCRP** meetings, where there is a set agenda which includes discussion on data controls, processing, issues and continual improvement.