Safer Business Network CIC Business Crime Reduction Partnerships [BCRP]

PERSONAL DATA PROCESSING DOCUMENTATION [Offenders]

This document describes the way that personal data is processed and secured by the BCRP as required by Article24 of GDPR.

1. **Definition of Data Protection terms**

a) **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. All data subjects have legal rights under the General Data Protection Regulation [and regional recitals] and the Data Protection Act 2018 in relation to their personal information.

b) **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, a unique reference number, address or date of birth) or it can be other information about that person, their actions and behaviour which, taken together, could identify that person.

c) **Data Controllers** are the people or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with GDPR.

d) **Data Processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it includes suppliers, providers and contractors which handle personal data on the BCRP's behalf.

e) **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using and viewing, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

f) **Special Category Data** (previously known as "sensitive personal data") includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. The definition also includes the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation. Special Category Data can only be processed under strict conditions. Personal Data relating to criminal convictions and offences is subject to additional requirements and should be handled in a similar way to Special Category Data.

g) **Third Party** - Any individual/organisation other than the data subject, the data controller or its agents.

h) **Data Protection Impact Assessment** is a process to help identify and minimise the data protection risks of a project. A DPIA should be carried out for processing that is likely to result in a high risk to individuals. The DPIA must: describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks.

2. **Contact details**
Safer Business Network CIC
PO Box 5398
Brighton BN50 8GQ
Email address: companysec@saferbusiness.org.uk
Tel: 01273 733393

3. The BCRP's Data Controller is the board of directors of the Company and they are responsible for ensuring compliance with current data protection law. The BCRP's Data Protection Officer [DPO] is the Company Secretary and both the DPO and the Data Controller can be contacted at the above address or email address. The BCRP scheme is registered with the Information Commissioners Office as a Business Crime Reduction Partnership[1].

The JAPAN test

4. Before data processing occurs it will be subjected to the JAPAN test shown below:

Justification	Can we justify the need to collect/store/share/destroy the personal information we are handling?
Authorisation	What authority are we using to do this? What is our legal basis?
Proportionality	Is what we are doing proportional to the purpose? Could we achieve the same purpose by recording or sharing less or no personal information?
Audit	Do we have a record of what we have shared, with whom and why, so that there is evidence [an audit trail] of our actions?
Necessary	Is what we are doing necessary or can the end result be achieved in some other way?

Types of Data Subjects processed

5. The Scheme processes the personal data of:
'Offenders': individuals aged 14 years and over who have been reported to have been actively involved in incidents which have presented a threat or damage to the property or safety of Members of the BCRP or Members' staff or customers or disrupt the peaceful enjoyment that their customers expect from the goods and/or services that our Members offer.

Purpose of processing personal data

6. Members of the Scheme have the right [a legitimate interest] to protect their property, staff and customers from crime and anti-social behaviour and to exclude from their premises any individuals who are proven threats to their property, staff or customers or disrupt the peaceful enjoyment that their customers expect from the goods and/or services that our Members offer. The scheme processes offenders' personal data for the specific purposes of managing its Exclusion Scheme on behalf of its Members, to draw active offenders to the attention of our Members and inform them of an offender's modus operandi, to collate intelligence on criminal activity within the area of the

[1] Registration number Z2662061

scheme's operation and to contribute to legal proceedings against offenders where appropriate.

7. The scheme's area of operation, and its Exclusion Scheme, is within the boundaries of the city of London.

Lawful Basis of Processing
Legitimate Interest

8. The scheme's Members' 'legitimate interests' provides the lawful basis on which it may process specific items of offenders' personal data for specific purposes without the offenders' consent.

9. The scheme has assessed the impact of its processing on offenders' rights and freedoms, has balanced these with its Members' own rights, and has concluded that its Members' rights prevail over Offenders' rights in this specific matter. This means that, for the specific purpose of managing and operating the business crime reduction partnership including addressing the issues of crime and disorder and the administration of its Exclusion Notices under the lawful basis of 'legitimate interests' it can therefore process offenders' personal data without requiring their consent [see the Legitimate Interests Assessment at paragraph 58].

10. When an offender is reported by a Member or partner agency for participating in any threat or damage to any Member's property, staff or customers or disrupting the peaceful enjoyment that customers expect from the goods and/or services that our Members offer, the information received will be subjected to a confidence test shown below:

Intelligence Assessment		Source Evaluation: *Reliable*	*Untested*	*Unreliable*	
High confidence	**ed to be False**	**LOW**	**LOW**	**LOW**	
	Authenticity Unknown	**LOW**	**LOW**	**LOW**	
Medium confidence	**Known**	**MEDIUM**	**LOW**	**LOW**	
	Authenticity Directly Known	**HIGH**	**MEDIUM**	**LOW**	
Low confidence	**t corroborated**	**HIGH**	**HIGH**	**MEDIUM**	

11. The **source evaluation** will fall into one of three categories:

    a. **Reliable** – This is only used when there is no doubt as to the authenticity, competence and reliability of the source. This grading may include technical information sources e.g. surveillance video, or a source which has consistently proven reliable in the past e.g. police officers, Members who report regularly and who have proven reliable previously or actual witnesses at the scene.
    b. **Untested**– Sometimes it will not be possible to make an informed decision as to sources reliability. This does not mean that it cannot be used, but is treated with caution and must be corroborated with more reliable or additional information if possible.
    c. **Unreliable** – This is never processed

12. The **intelligence assessment** will fall into one of five categories:

a. **Known to be true without reservation**. This information will often be collected by technical surveillance or witnessed first-hand by BCRP staff. A report that is hearsay cannot fall into this category.
b. **Known personally to the source but not to BCRP staff** –Information is second hand such as information from a witness relayed by a Member.
c. **Not known personally to the source but corroborated by information already recorded** – This is information that has been passed to a source from a third party, but is backed up by other information e.g. CCTV footage.
d. **Not known personally to source and cannot be corroborated** – This is when the source has received the information, but there is no way of cross referencing it to other information or other means of corroboration. The reliability of this information cannot be judged, and it cannot be processed.
e. **Suspected to be false or malicious** – This information is known or suspected to be deliberately untrue. It cannot be processed.

13. Once data is processed it will be stored in secure Cloud-based databases which are certified to the Cyber Essential Standard. BCRP databases have two parts:

i) a restricted section accessible only to authorised BCRP staff and

ii) an open section available only to BCRP Members and partners via computer or mobile phone app on a need-to-know basis. This part is password protected.

Full details of incidents reported by our Members and partners in addition to personal data will be stored in the restricted section. Very limited data are available in the open section e.g. name, photograph and brief details of the offence for which the offender is known. Where appropriate, details of conditions imposed by law enforcement bodies may also be shown.

Vital Interest

14. At the request of a law enforcement agency, SBN may process and share with its Members details of missing persons under the lawful basis of 'vital interest'. Only a name and photographic image will be shared and such data will have an expiry date of 10 days. No data will be retained.

Substantial Public Interest

15. Applied in the case of Sexual Risk Orders [SRO] [including Interim Sexual Risk Orders] under DPA Schedule 1, paragraphs 6-28, where the details of conditions and restrictions associated with an SRO can be circulated to Members to:
    a. prevent or detect unlawful acts
    b. protect the public
    c. safeguard children and individuals at risk

16. As a safeguard, the sharing of such data with Members will be subject to consultation with the appropriate public body [MPS] and will require written approval at a minimum of Inspector level. Such data will have an expiry date no later than the expiry of the SRO.

Categories and types of personal data processed

17. **Offender's name, date of birth and facial image** being a picture made using a camera and/or video footage of an offender captured on closed circuit TV system[s] without any prior or subsequent specific technical processing. The purpose of this data processing is to enable Members to identify offenders in order to fulfil the requirements of an Exclusion Notice and/or submit reports about

them and/or to include them in a list or gallery of offenders and excluded persons (if appropriate) and to protect the personal safety of Members and their staff, customers etc.

18. **Offenders' postal and email addresses, telephone number(s) and other contact details**; the purpose of this processing is to enable the scheme to inform offenders of the data we hold about them under Article 13 of GDPR. We may also send confirmation of exclusions, rules of the exclusion scheme, or warning letters. Offender's contact data is not the property of the BCRP and will not be shared with Members.

19. **Information and evidence about alleged incidents in which an offender has been involved**; the purpose of this processing is to enable the Scheme to assess the suitability of an exclusion notice against the offender and to defend its legal rights against any claim or suit by an offender or other party. Detailed data may be processed but will not be shared with Members; rather a two or three word summary description of the general offence for which the offender is known e.g. 'theft' or 'fraud'. Details of such data may be shared with the Scheme's Data Controller and Board of Management as necessary and also in the course of any legal proceedings.

Special Category Data

20. In order to lawfully process special category data, GDPR makes it clear that an organisation must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

21. The processing of special category data is allowed under UK derogations for the purposes of the prevention of crime and disorder – DPA2018 Schedule1, Part 2, 10(a).

22. The processing of special category data will be avoided if possible but any such processing will 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 [Article 9. 2(g)].

23. The following table shows in detail what data will be processed, with whom it will be shared and the reason for distribution:

Category	Processed?	May be shared with?	Justification
Name	May be processed.	Members. Other accredited BCRPs in SBN's ROCU[2] area[3]. Police[2]. Other public sector and charitable bodies[2].	To allow the BCRP Members and other parties listed to identify excluded individuals and submit reports about offending behaviour.
Date of Birth	May be processed.	Members.	To allow the BCRP members and other parties listed to

[2] Regional Organised Crime Unit

[3] Subject to an extant DSA

		Other accredited BCRPs in SBN's ROCU area. Police. Other public sector and charitable bodies.	correctly identify excluded individuals [especially in the night-time economy] and submit reports about offending behaviour.
Photographic [still] Image	May be processed.	Members. Other accredited May be shared with BCRPs in SBN's ROCU area. Police. Other public sector and charitable bodies.	To allow the BCRP Members and other parties listed to correctly identify excluded individuals and submit reports about offending behaviour.
Moving image video footage	May be processed	Will not be shared with Members or charitable bodies. May be shared with other accredited BCRPs in SBN's ROCU area. May be shared with police.	To identify travelling offenders. To assist a law enforcement agency in evidence gathering.
Alleged Offences against our members	May be processed.	Members but will not be shared in detail. Only a brief [two or three word] description of the offences for which the offender is known.	To allow Members and other parties listed to assess risk.
Race	Will not be processed.	Will not be shared.	
Ethnic origin	Will not be processed.	Will not be shared.	
Politics	Will not be processed	Will not be shared.	
Religion	Will not be processed.	Will not be shared.	
Trade Union Membership	Will not be processed.	Will not be shared.	
Genetic data	Will not be processed	Will not be shared.	
Biometric data	Only a photograph[4] taken with a camera and not subject to any specific technical	Members.	For the purposes of assisting BCRP

[4] A photograph was deemed to be biometric in the Judicial Review of M vs Chief Constable of Sussex but this is contested by other sources

	processing may be processed. No other biometric data will be processed. Photographic images will be security seeded to enable identification of the Member involved if data integrity is breached.	Other accredited BCRPs in SBN's ROCU area. Police. Other public sector and charitable bodies.	Members and other parties listed to identify excluded individuals.
Health data	Will not be processed.	Will not be shared.	
Sex life	Will not be processed.	Will not be shared.	
Sexual orientation	Will not be processed.	Will not be shared.	
Criminal convictions	Alleged criminal offences against our Members will be processed under Schedule 1, Part 2, Para 10[a] of DPA 2018. Conditions attached to Criminal Behaviour Orders [CBOs] and Community Protection Notices [CPNs] will be processed under Schedule 1, Part 2, Para 10[c] of DPA 2018	Members. May be shared with other accredited BCRPs in London with which we have a DSA. Police.	To inform members of the potential offence they can expect from an offender. To assist in monitoring compliance with CPNs and bail conditions and report any breaches in the interests of the prevention or detection of crime.
Radio transmission voice files	May be processed.	Will not be shared with Members or charitable bodies but may be returned to the original owner. May be shared with police.	To assist a law enforcement agency in evidence gathering.
Offender's Bail Conditions	May be processed.	May be shared with Members[5].	The prevention or detection of crime Safeguarding children and vulnerable adults
Offender's Sexual Risk Order Conditions & Restrictions	May be processed	May be shared with Members subject to consultation with appropriate public body.	The prevention or detection of unlawful acts.

[5] Precedent established in the Judicial Review of M v Chief Constable of Sussex that bail conditions of juveniles can be shared with BCRP Members who, by virtue of their BCRP membership, are not deemed to be 'members of the public'

			Protection of the public Safeguarding of children and individuals at risk
Offender's Address	May be processed.	Will not be shared.	To comply with the requirement of Article 13 to inform the data subject of the personal data we hold.

24. **Sources of personal data**

a. **Offenders** themselves who may voluntarily offer information about themselves;
b. **Members** who may submit reports about incidents in which offenders have been involved. They may also send relevant 'intelligence' about offenders, for example they may provide a name when asked to identify an unidentified CCTV image.
c. **Other business crime reduction partnerships** or similar accredited private sector agencies with which we have a formal data sharing agreement if an offender is suspected of travelling to offend.
d. **Police or other public agencies** may provide offenders' personal data under a formal Data Sharing Agreement.
e. **Offender's social media platforms** may provide information that is in the public realm by virtue of being displayed without privacy controls on a publicly accessible platform.

25. If the data passes the confidence test, points will be allocated to the reported offence. The points [shown below] are based on Criminal Sentencing Guidelines:-

Aggressive behaviour or verbal abuse – No mitigating factor/assault	**1**
Anti-social behaviour – any behaviour causing harassment, alarm or distress to staff or patrons of member premises	
Attempted theft	
Breach of Section 35 or CPO	
Criminal Damage leading to minor financial loss	
Drunk & disorderly in or around member premises	
Ejected from a venue for refusing to leave	
Fraudulent use of ID [user or supplier]	
Theft from premises under £200	
Suspected Possession of Drugs inside member premises	
Possession of stolen goods from other member premises	

Breach of a CBO	**2**
Breach of CPN [if relevant to our members' interests]	
Fraud under £200	
Going Equipped	
Theft from Premises over £200 but under £1000	

ABH	**3**
Burglary of member premises	
Breach of a BCRP Exclusion Notice – Length of ban to be extended from date of breach.	
Common Assault	
Criminal Damage of Member premises leading to significant financial loss	
Fraud over £200	
GBH	
Suspected Possession of drugs with intent to supply with additional circumstantial evidence	
Possession of an offensive weapon	
Robbery	
ABH	
Burglary of member premises	
Racist or homophobic abuse	
Sexual Assault	
Theft from person in or around member premises	
Threats to kill or harm	
Verbal or physical aggression/threats of violence towards staff	

26. A points threshold will determine further actions as shown below:

Threshold for a warning letter to be sent to the offender together with a privacy statement and details of appeal procedure.	1 point

Threshold for bringing an offender to the attention of Members via inclusion on the Member-facing database and app.	
Threshold for Exclusion from Members' venues and an exclusion notice to be sent to the offender together with a privacy statement and details of appeal procedure. Offender's data will be shared on the Member-facing database. Threshold for formally sharing offender data with Police as a persistent offender.	3 points

Mitigating Factors

- Any incident involving a racist, homophobic, misogynistic element, or is discriminatory towards religion or disability can be upgraded to an Exclusion notice if the initial offence does not meet the points criteria.
- Any incident that is accompanied by a threat of violence can be upgraded to an Exclusion Notice
- An offender's vulnerability due to Mental Health conditions can be considered if confirmed through a statutory partner (Police or Local Authority)
- Safer Business Network may process or exclude juvenile offenders but does so judiciously. Exceptions can be made for persistent and prolific offenders who are causing a significant impact on member premises or juveniles involved in gang-related activities.

Sharing data

27. Data may be shared with:

    a. **Members** who are business and/or property owners, their agents or their employees working within the operational area of the scheme who share the same legitimate interests.
    b. **Employees and officers of public agencies involved in the prevention and detection of crime**, such as police and relevant local authority departments whose lawful basis for processing offenders' data is their public task.
    c. **Charitable organisations** also involved in the prevention of crime and public disorder subject to a data sharing agreement.
    d. **Data Controllers of other organisations**, similar in nature to the scheme, in neighbouring areas [but within SBN's ROCU area] if there is evidence that an offender has participated in any threat or damage to property, staff and customers in areas outside the BNCRP's area of operation.

28. The BCRP will not transfer offenders' data outside of the UK.

Data retention period

29. If the data fails the confidence test it will be immediately irrevocably destroyed without any further processing. If it passes the confidence test and meets the points criteria for being brought to the attention of our Members it will be available on the Member-facing, open database for a maximum

of 13 weeks if no further reports are received.

30. If it meets the points criteria for exclusion, the offender's name, date of birth, facial image and the offence for which they are known may be shared among Members on the Member-facing database for a maximum of 12 months or the full term of any relevant court imposed sanction. If no further report is submitted during that period, the offender's profile on the open database will be deleted without delay.

31. If, during the 12 months when an offender is excluded, they commit further incidents involving a threat or damage to any Member's property, staff or customers, *and* they reach the appropriate threshold, their exclusion may be renewed and their name, facial image and date of birth may be circulated among Members on the open database for a further maximum of 12 months from the date of the further report. If no further report is submitted by a Member or public agency during that period, the offender's data will be withdrawn from the open database at the expiry of that period. It will be retained for a further maximum of 12 months [6 months for offenders under the age of 18] in the BCRP's closed database [which can only be accessed by authorised personnel] after which it will be irrevocably deleted.

32. Personal data may also be transmitted via the radio networks operating in the city. All radio transmissions will be recorded on the BCRP's radio management system and will be stored for a period of 28 days after which they will be erased. They will be shared with law enforcement agencies upon request to support the investigation of a crime and the original owner of any transmission may request a copy [.wav file] for their own internal processing purposes.

Data Processors

33. The Scheme employs the services of the following Data Processor(s) under contract as required by DPA2018 Part 3, Section 59(5):
    a. **Littoralis Limited**;
    b. **SentrySIS Ltd**

Standard Operating Procedures

34. The following Standard Operating Procedures have been defined relating to the processing of personal data by the BCRP and in compliance with current data protection law:

Documentation management

35. Every twelve months the Data Protection Officer will review all documentation relating to the management of personal data, including the Scheme's *Privacy Notices* (Offenders and Members), *Personal Data Processing Documentation*, *Legitimate Interests Statement, Data Protection Impact Assessment(s)* and, where relevant, Information Sharing Agreement(s) and Data Processing Agreement(s).

36. Where any revision is necessary, a new version of the relevant document will be created to replace the previous version (which will be retained by the Data Controller).

37. Where it is necessary that Members re-certify against any revised document, the Data Controller will secure re-certification by all Members when they next access the scheme's data via the website or mobile phone app.

Subject Access Requests

38. Within 30 days of an applicant submitting a Subject Access Request to the BCRP the DPO must confirm its receipt with the applicant.

39. As soon as practical thereafter the Data Controller must satisfy itself as to the identity of the applicant; where necessary this may require identification in person by personal facial recognition or the presentation of a photo identification document.

40. As soon as practical thereafter the DPO must ensure an appropriate member of BCRP staff has:
    a. collected all personal data relating to the applicant, including image(s).
    b. redacted all data identifying any other person from the data.
    c. provided the relevant personal data to the applicant, in a conventional, readable format.
    d. provided documentation demonstrating the scheme's compliance with data protection law.
    e. informed the applicant of their right to require corrections of any data which the applicant can demonstrate to the satisfaction of the Data Controller is incorrect, unnecessary or disproportionate.
    f. documented the completion of the SAR process.

Reporting a Personal Data Breach [also refer to Data Breach Management Plan at paragraph 100]

41. Within 72 hours of becoming aware of a breach of personal data the Data Controller must report the breach to:
    a. the Board of Management.
    b. the Information Commissioner's Office if deemed sufficiently serious.
    c. any relevant Data Processor.
    d. any involved third party.

42. As soon as possible thereafter, in the case of a data breach which, in the view of the DPO, is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Data Controller must inform those individuals of the breach and the nature of the resulting risk to their rights and freedoms.

43. The Data Controller must document each Personal Data Breach in an Appendix at the end of this document.

Privacy Notices distribution

44. **Where data is collected directly from the Offender:** the Privacy Notice (Offender) must be served to the offender at the time and place of data collection. Use best endeavours to record the service of the Privacy Notice and retain a record of service.

45. **Where data is not collected directly from the Offender:** within five working days thereafter use best endeavours to serve a Privacy Notice unless the provision of such information proves impossible [Article 14, para 5(b) of GDPR] but as a matter of general principle, all exceptions to the right to be informed will be interpreted restrictively and applied narrowly. A record of service/delivery of the

Privacy Notice will be retained.

46. In any event, the Privacy Notice (Offenders) and this Data Processing Documentation in full will be displayed on the BCRP's website where it is publicly available to maximise the likelihood and possibility of access by offenders.

Registration of the Scheme with the Information Commissioners Office

47. Each year, at the notification to the Data Controller of the annual renewal of the Scheme's registration with the ICO, the Data Controller must review the BCRP's registration with the ICO.

48. As soon as possible thereafter, where the registration requires updating or revision, the Data Controller must communicate the proposed revision to the ICO's Registration department at registration@ico.org.uk .

Data Security

49. The BCRP will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

50. The BCRP will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

51. Personal data will only be transferred to a data processor that has provided sufficient guarantees to implement appropriate technical and organisational measures that will comply with data protection legislation and ensure that data subject's rights are protected and that these requirements are governed by a data processing contract or other legally binding agreement.

52. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

    a) confidentiality means that only people who are authorised to use the personal data should access it.
    b) integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
    c) availability means that authorised users should be able to access the personal data if they need it for authorised purposes.

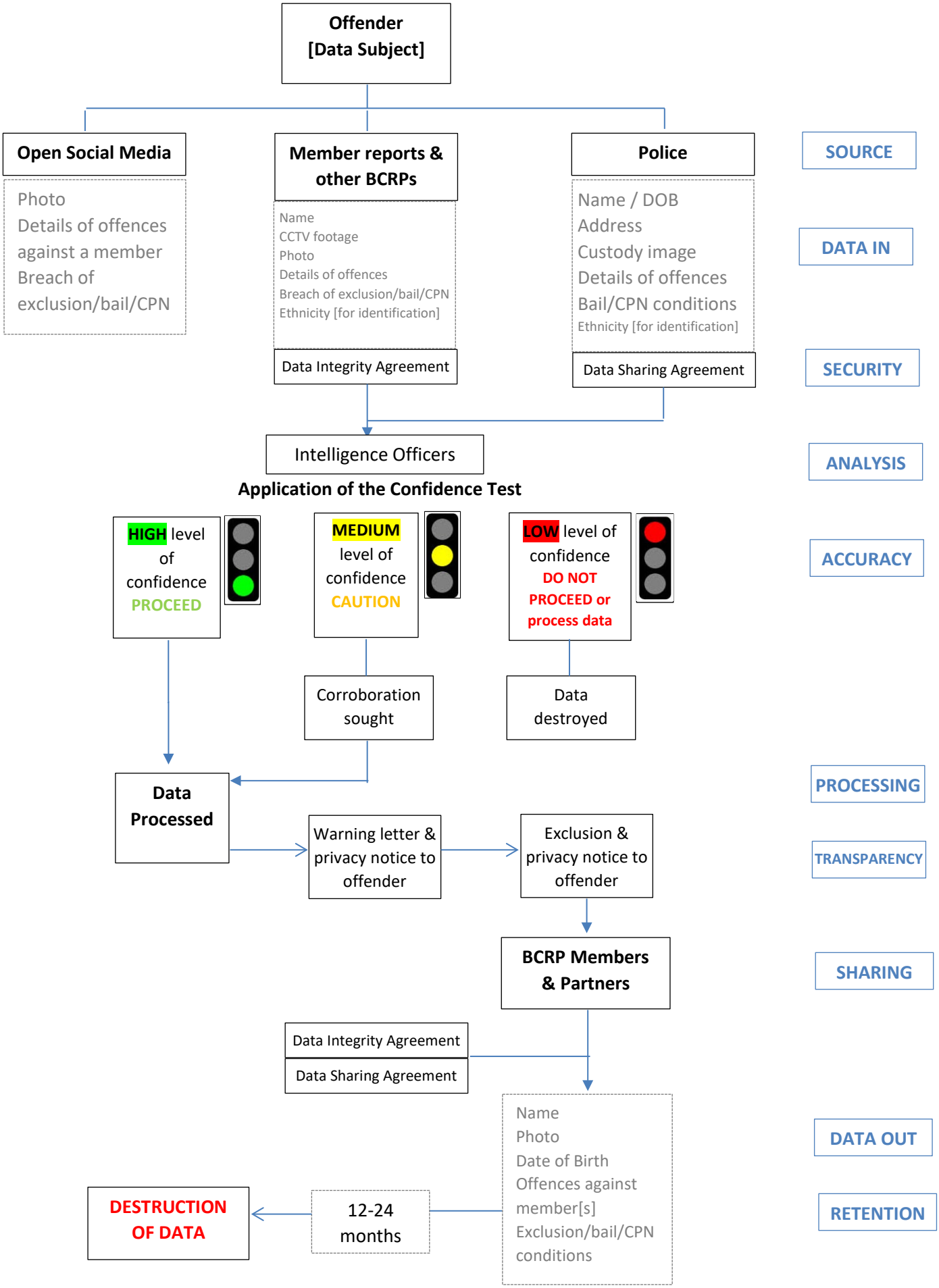
53. Security procedures include:

    a. Secure lockable desks and cupboards. Holding personal information in non-digital format is to be avoided but desks and cupboards will be kept locked if they hold confidential information of any kind [personal information is always considered confidential].
    b. Methods of disposal. Paper documents will be shredded. Digital storage devices will be physically destroyed when they are no longer required. Equipment such as PCs and hand-held devices will be password protected. BCRP employees will log off from their laptops when left unattended.

54. The BCRP processes all personal data within an online 'secure environment' in which all personal data processed by the scheme is secured. The system is ISO27001 accredited and aligns with the

principles of ‘Data Protection by Design and Default’ as defined in the latest version of the processors’ *Information Security Management and Policies*.

GDPR Data Flow Chart



Legitimate Interests Assessment [LIA]

55. **The Purpose**
The BCRP is a membership organisation administering crime reduction partnerships in various boroughs of the City of London to assist businesses to prevent crime and disorder. One of the services it offers to its members is an exclusion notice scheme which bans persistent offenders from member premises for a period of one year. The BCRP operates in both the day-time and night-time economies of the city. This affords our members the opportunity to avoid and/or prepare for interaction with individuals who threaten their right to peacefully offer their goods and services to members of the public without fear of anti-social behaviour, crime or disorder. Similarly it is advantageous to members of the public who have the right to purchase goods and services from our Members in a safe and secure environment.

56. The Members complete a written agreement that vests in the BCRP the authority to exclude individuals from their venues on their behalf. Details of excluded individuals are then made available to Members via a secure, encrypted, password-protected intranet accessed via desktop and laptop computer or a Smartphone app.

57. Members report incidents about offenders' criminal and/or anti-social behaviour to the BCRP and such reports are subject to a confidence test [see paragraph 10] and allocated points [based on Criminal Sentencing Guidelines]. Details of the offence and limited personal data are processed on secure databases. As soon as a report is received, and assuming it passes the confidence test, wherever possible the individual is contacted in writing [a warning letter] to inform them that they are in danger of being excluded together with an accompanying formal privacy notice [which is also available on the company's public facing website]. Subsequent offending behaviour may result in the threshold being reached for exclusion and offenders are then informed of their exclusion in writing with another accompanying formal privacy statement.

58. Once excluded the offender's name, date of birth, photograph and a brief [two or three word] description of the offences against our members for which they are known is placed on a database that is made available to Members. The purpose of making this limited personal data available to Members is to enable them to identify the offender and ensure they are excluded from their venues and to assess the risk that the offenders pose. The persons most likely [though not exclusively] to need to have the data will be security staff, registered with the Security Industry Agency, essentially responsible for enforcing the exclusion notice.

59. Individuals are solely excluded from the premises of BCRP Members and their data is only shared with Members within the city of London.

60. The BCRP processes offenders' personal data for:
    a. the specific purpose of managing its Exclusion Scheme on behalf of its Members.
    b. to inform Members of an offender's modus operandi and enable them to assess risk.
    c. to collate intelligence on criminal activity within the area of the BCRP's operation
    d. to contribute evidence to legal proceedings against offenders where appropriate.
    e. to detect and prevent crime and anti-social behaviour.

61. The processing benefits:
    a. businesses in the day-time and night-time economies that are better prepared to address issues of crime and anti-social behaviour and to deter repeat offenders.
    b. members of the public who are made safer by the reduction in crime and anti-social behaviour.
    c. the offenders themselves who often cease to offend upon receipt of a warning letter [a study by Gloucester University found that 76% of offenders in receipt of a BCRP warning letter do not reoffend [6]].
    d. law-enforcement agencies that gain additional intelligence from member businesses and resources from the BCRP and a platform to deliver advice and guidance.

62. Business Crime Reduction Partnerships are now commonplace with over 250 operating in the UK[7] They are highly valued by businesses and law-enforcement agencies and are recognised nationally. In 2018, the National Business Crime Centre devised a common accreditation scheme for BCRPs[8] under the auspices of Secured By Design. In addition the National Association of Business Crime Partnerships [NABCP] is an umbrella body recognised by the Home Office.

63. The principle purpose of processing personal data is the administration of an exclusion notice scheme and the deterrence of crime and anti-social behaviour. The BCRP processes hundreds of Member reports every year. If this was prevented the scheme could not operate and there would be neither an intelligence gathering resource for persistent offenders nor any mechanism for coordinating their exclusion from multiple business premises. Individual premises could issue individual exclusions but the effect of exclusion would be severely diluted. In addition, there would be no mechanism for informing business owners and security personnel about offenders who are likely to commit crimes in their premises or the modus operandi of prolific offenders to inform in-store improvements in security systems.

64. The BCRP is registered with the information commissioner[9] and complies with the Data Protection Act 2018 and is a member of the NABCP. A Data protection Impact Assessment as required by Article 35(1) has been completed and is included in this documentation at paragraph 99. The BCRP's actions also take into account Section 6 of the Crime & Disorder Act 1998 and Article 8 of the European Convention on Human Rights.

Necessity

65. The overall crime rate in London between March 2020 and March 2021 was 83.3 crimes per 1,000 people with theft and handling and violence against the person having the highest incidence. The full range of crimes and their distribution by London borough can be found at https://www.met.police.uk/sd/stats-and-data/met/business-crime/ .

66. The retail trade body, the British Retail Consortium (BRC), says there were on average 455 incidents of abuse of shop staff a day in the UK as a whole in 2019, up 7% on the previous year. In 2020,

[6] Business Crime Reduction Schemes: An examination of operation, management and best practice. Univ of Gloucester. 2019
[7] National Association of Business Crime Partnerships 2020
[8] https://nbcc.police.uk/guidance/bcrp-standards-latest-version
[9] Registration number Z2662061

a survey of the UK's top 100 retailers, carried out by law firm TLT, found that a nearly a third (31%) of retailers had experienced abuse against shop workers. Many surveys of retail crime rely on information about reported crimes and cannot take into account unreported crime so the problem is likely to be larger than portrayed. The need to address issues of crime and disorder is evident from the figures above. The Gloucester University study[5] demonstrated the success of BCRPs in reducing offending with 76% of offenders in receipt of a BCRP warning letter ceasing to reoffend.

67. The retail and leisure areas of London's boroughs are the geographical centres for much of the city's crime and disorder and they are the main areas of operation in the boroughs where SBN operates a BCRP.

68. The financial impact of crime is significant. Business crime, excluding fraud and cyber-crime, accounts for 17% of all reported crime nationally and the cost to the UK is over £614m per annum[10]. Crime is costing retailers increasing amounts of money every year, amounting to a total of £2.2 billion in the UK alone. This amount includes money directly lost through crime along with retailer's spend on loss prevention in 2020 [11]. Estimated costs of crime have been provided by the Home Office[12] and cover, for example, physical/emotional harm, lost output, value of property stolen/damaged, and the cost of health, police and other public services in response to crime. Estimated average costs include:
    a. £14,100 for a violent crime with injury/£5,900 without injury.
    b. £5,900 for a domestic burglary.
    c. £1,400 for other criminal damage.
    d. £39,400 for rape and £6,500 for other sexual offences.

69. Tackling anti-social behaviour is a principle activity of the BCRP and it is also a priority theme of the MOPAC Police and Crime Plan 2017 - 2021. The paragraphs above demonstrate at the macro level the need to process data to address issues of crime and disorder. On a micro level the need to process and share data is to enforce the exclusion notice scheme and assist Members to address issues of crime and disorder. The processed data will not be used for any other purpose.

70. The processing of personal data of alleged offenders without their consent is proportionate as outlined in Article 6(1f) of GDPR and Schedule 1, Part 2, 10(a) of DPA18 which allows the processing of personal data for the prevention and detection of unlawful acts.

71. The proportionality is further supported because the issue being addressed is large [crime and anti-social behaviour in the city] but the degree of data processing is limited and the sharing of personal data is even more limited. Members are only able to access four personal data elements:
    a. Name of the offender.
    b. Photographic image [without specific technical processing].
    c. Date of birth.
    d. A brief description of the alleged offence(s) against BCRP members for which the offender is known and conditions applied by a court if appropriate.

[10] MOPAC 2020

[11] Centre for Retail Research 2020

[12] The economic and social costs of crime, Home Office, 2018

72. The table at paragraph 18 shows the full range of data that is processed and with whom it will be shared. Extra care is given to avoid processing sensitive personal data. It is the opinion of the BCRP that the very minimum of data is processed to achieve the objectives of the scheme and there would be no other way to achieve the same end by other means or by processing less data. An exploration of the alternatives is shown below:

Current Processing	Possible Alternative	Conclusion
Incident reports of alleged offences against Members.	Do not ask Members to report incidents to the BCRP.	There would be no basis to operate the exclusion notice scheme and warning letters would not be issued and our Members would be disadvantaged. There would be one less mechanism to reduce offending and reoffending. There would be less intelligence available to the police to assist with strategic decisions on the allocation of resources.
Photograph of offender.	Do not process or share this data.	It would be impossible for Members to accurately identify offenders which may lead to mistaken identity or offenders continuing to offend in member venues. *"An exclusion scheme of the type operated by the BCRP in the public interest would patently be unworkable without an image enabling the excluded person to be identified."* **Lady Justice Andrews. Court of Appeal: Case No: C1/2019/2622 & C1/2019/2623 17.12.20.**
Date of birth of offender.	Do not process or share this data.	It would be more difficult to accurately identify offenders and/or to submit reports to the police. Licensed night-time venues often require proof of DOB for entry to their premises.
Name of offender.	Do not process or share this data.	It would be difficult to accurately submit reports about offenders.
Alleged offences against Members for which the offender is known.	Do not process or share this data.	Members need to know the broad types of offence they may encounter when an offender is in their venue e.g. theft, fraud etc. This may also be important to assess risk when they request that the offender leave their venue e.g. if the offender is known for violence.
Data is retained for the duration of the exclusion notice period [12 months].	Delete data immediately when an exclusion notice is issued.	Data is only accessible to members between 13 weeks and 12 months unless further intelligence about criminal activity or anti-social behaviour is submitted to the BCRP, or the individual is already subject to an exclusion notice. Upon exclusion data may be required for the appeal process which can occur any time during the exclusion term. Data may also be required if

		further reports of offences are received during the exclusion term.

Balancing Test

73. No sensitive personal data is processed or shared with Members. A photograph taken with a camera and not subject to any specific technical processing is processed, which some sources[13] consider to be biometric data. This is disputed but in any event, no other biometric data is processed.

74. Data about criminal offences are not held in a 'comprehensive register' [Article 10] and is permitted under Schedule 1 of the DPA18 – preventing or detecting unlawful acts and protecting the public against dishonesty. Data are limited to:
    a. bail conditions.
    b. conditions imposed by Community Protection Notices.
    c. Criminal Behaviour Orders.
    d. alleged offences committed directly against our Members.

75. Individuals are likely to consider this information private, especially data listed in paragraph 74 above [criminal offences]. However, court bail conditions, CPNs and CBO's are issued in open court and consequently could be in the public domain. In addition members of the BCRP do not receive the information as 'members of the public' but in a private capacity, subject to contractual and other constraints limiting its use and precluding it from coming into public circulation.[14]

76. Apart from issuing a warning letter which also informs individuals about the data that the BCRP holds [via a privacy statement and the possibility of an exclusion notice being served], the BCRP has no direct relationship with the individual. It is made clear, however, that there is an opportunity to appeal against the process and the BCRP informs the individual how they can complain to the ICO.

77. Reported incidents which may contain personal data are subjected to the confidence test and are processed within five working days or irrevocably destroyed if they fail the test. Where possible, the warning letter/privacy statement is also sent within five working days and it ensures that the individual knows exactly what information we hold, what we intend to do with it, how long it will be kept and with whom we will share it. It also offers the individual the opportunity to avoid further action by ceasing to offend. The warning letter has a reading age of 10 and is intended to be understandable by any age group.

78. Once processed, data is only shared with organisations for which it is relevant and the minimal amount of data is shared to fulfil the purposes set out in this documentation.

Impact of processing

79. The processing of personal data will only impact the individual directly if they reach the threshold for being raised to our Members or exclusion. In the event of being excluded some of their personal freedom will be removed in that they will be banned from entering some business premises but limited only to BCRP Members' premises. In the totality of the entire city this is a very small number

[13] Justice Lieven in Judicial Review of M v Chief Constable of Sussex Police 2019 deemed a photograph to be biometric
[14] A view supported in Justice Lieven the Appeal against M v Chief Constable of Sussex Police

and the curtailment of their freedom is considered to be slight.

80. Some people may find this data processing by the BCRP intrusive but it is proposed that an individual engaged in criminal activity in a business premises would expect to surrender a small amount of personal data upon discovery and detention by security personnel or the police e.g. name, address, date of birth. In addition it is increasingly normal for their image to be captured on CCTV or other recording devices with their tacit consent. In this sense they should not be surprised by the processing of their data brought about by virtue of their offending. Their rights under Article 21 are not affected.

81. The entire procedure of data processing is freely available on the BCRP's public facing website and details are available to anyone who enquires by phone or email. The website also has a Frequently Asked Questions page devoted to exclusion notices and a separate page for data protection with answers provided in easily understood 'bite-size' question & answer format as recommended by the ICO.

Safeguards

82. The individual is not in a position to control their personal data but its dissemination is limited in scope and distribution and the following safeguards will be employed to protect their rights:
    a. The default position is not to exclude individuals in which case their data need not be processed.
    b. Only BCRP staff vetted to NNPV Level 2 or DBS vetting will be allowed to process data.
    c. The number of BCRP staff with access to reports from members will be strictly limited to those responsible for data processing.
    d. The application of the confidence test will ensure accuracy.
    e. The application of a points based threshold for data sharing with Members will ensure fairness.
    f. The data subject will be informed of any data processing and the appeal mechanism within five working days of receipt of data from any source.
    g. The minimum amount of data will be shared with Members.
    h. Sharing of data with Members will be subject to a strict data integrity agreement with sanctions in place to punish any breach.
    i. A mechanism is in place [security seeding] to identify the individual Member responsible for any breach.
    j. Members will not be granted automatic access to the database holding personal data about offenders and checks are put in place to verify the identity of applicants and their bona fides as BCRP Members.
    k. Members with access to the open database are reviewed every 13 weeks and those who have not logged on during that period are deleted.
    l. Members with access to the BCRP database are required to re-certify acceptance of the data integrity agreement every 13 weeks.

Children's data processing

83. The General Data Protection Regulation [GDPR] does not ban an organisation from relying on legitimate interests as a lawful basis for processing children's personal data. However, the GDPR places particular emphasis on the need to protect the interests and fundamental freedoms of data

subjects when they are children.

'Processing will be lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or 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.'***[15]

84. In terms of safeguarding, children are unlikely to come into direct contact with any of the BCRP staff; the BCRP does not arrange any events or activities involving children. But they may be affected by some of the services that we offer to our Members, specifically the exclusion notice scheme. We recognise The Children Act 1989 and the Children Act 2004 and believe that children and young people should never experience abuse of any kind and that everyone has a responsibility to promote the welfare of all children and young people, to keep them safe and to protect them from harm. In addition, some children will be especially vulnerable because of the impact of previous experiences, their level of dependency, communication needs or other issues and extra safeguards may be needed to keep these children safe.

85. The BCRP recognises Recital 38 which states that children require specific protection with regard to their personal data because they may be less aware of the risks and consequences of the processing, the safeguards that could be put in place to guard against these, and the rights they have. It also recognises Article 21 giving the right of the individual [or in the case of children the parent or guardian] to object to said data processing and for this reason *both* the child *and* the parent/guardian are informed of the processing within five working days of receipt of data.

86. Children are identified as "vulnerable individuals" and deserving of "specific protection" but, while UK derogations allow the processing of such data for the purposes of the prevention of crime and disorder, the definition of the age beneath which a person is considered to be a child is a confusing picture.

87. The United Nations Convention on the Rights of the Child requires countries to set a minimum age "below which children shall be presumed not to have the capacity to infringe penal law". However, the convention does not actually indicate what age level should be set as a minimum. But, when fixing a minimum age, it draws attention to the commentary on the United Nation's Beijing Rules which state that: "The modern approach would be to consider whether a child can live up to the moral and psychological components of criminal responsibility; that is, whether a child … can be held responsible for essentially antisocial behaviour."

88. Developmental psychologist Lawrence Kohlberg postulated that between the ages of 10 to 12 children learn "ideal reciprocity," which is the idea of fairness and 'right from wrong'; they can see things from another viewpoint and realize how some rules are concrete.

89. The age at which a child could not be held criminally responsible is encapsulated in the Latin term doli incapax which has been interpreted to mean 'incapacity of committing an offence'.

[15] Article 6 (1)(f)

90. Until 1998, the legal presumption (doli incapax) was that children aged under 14 did not know the difference between right and wrong and were therefore incapable of committing an offence. However, in response to the outcry over the Jamie Bulger murder, the doli incapax presumption was abolished by section 34 of the Crime and Disorder Act 1998 and is no longer in operation; in England & Wales 10 years of age is the lower threshold of criminal culpability.

91. This leaves England and Wales with one of the lowest age levels of criminal responsibility in the world and subject to ongoing criticism by the international community. Even England's closest neighbours, Scotland and Ireland have a limit of 12 years of age.

92. In 1995 the UN Child Rights Committee (UNCRC) presented its first report on the UK's compliance with the international child rights standards that the country had signed in 1989. It included a recommendation that a threshold below the age of 12 is not internationally acceptable, and that 14-16 years would be more in line with UNCRC Article 40 which specifies that States should deal with children in conflict with the law without resorting to judicial proceedings.

93. In an interview with the Times in March 2010 the Children's Commissioner Maggie Atkinson called for the age of criminal responsibility to be raised to 12 saying: "The age of criminal responsibility in this country is ten – that's too low. In some European countries it is 14". This is a view that is supported by the Children's Commissioner for Scotland who has stated publicly that Scotland should work incrementally towards a minimum age of criminal responsibility of 14 or even 16 years.

94. It is the belief of the BCRP that the age of 10, or even 12, is too young to fully understand criminal culpability. A recent survey of 90 countries found that the most common age [adopted by around a quarter of the sample] is 14 years.

95. There is some evidence that the English courts consider a child of 14 to be old enough to accept the consequences of their actions.

    a. In November 2021 a 14-year old was jailed for at least 16 years for the murder of Keon Lincoln in Birmingham.
    b. The two children found guilty of the fatal stabbing of Oliver Stephens in Reading in January 2021 were aged 13 and 14. They were both sentenced to 13 years in a young offender institution. An accomplice, who lured Stephens to the scene but did not participate in his murder, was also 14 years of age and was sentenced to 12 years.
    c. The case of a 14 year old Darlington schoolboy, who was not identified in court, found guilty of terrorism offences under section 58 of the Terrorism Act (2000) in January 2022.
    d. Craig Mulligan was sentenced to a minimum of 15 years in jail in June 2022 for the murder of Logan Mwangi. Mulligan was 13 at the time of the offence and 14 when sentenced.

96. Taking into account the age-appropriate rights and freedoms of the child so that their freedom to learn, develop and explore is only restricted when this is proportionate the BCRP will adopt the age as proposed pre-1998 as the minimum beneath which a child may not be fully aware of right and wrong and the consequences of their actions. Fourteen years of age will be the threshold beneath

which we will not process offender data.

Safeguards

97. The BCRP will be cognisant of the impact that data sharing/exclusion could have of the child's public image as they grow older. The following additional safeguards will be adopted to protect the rights of children between the age of 14 and 17:
    a. No data will be processed for children under the age of 14 but in the interests of safeguarding any information received will be passed on to the appropriate safeguarding authorities and then deleted.
    b. The default position is for children not to be excluded but diverted to other options which would result in their data not being shared with BCRP members at all.
    c. The child *and* the parent/guardian will be informed of any data processing and the appeal mechanism within five working days of receipt of data from any source.
    d. As required by Recital 39 any information given to the data subject will be easily accessible and easy to understand, using clear and plain language.
    e. There will be no automatic exclusion upon reaching the threshold. The decision to issue an exclusion notice will be subject to a meeting of the Board of Management consisting of a minimum of 3 people one of whom must be the CEO or the Crime Manager to ensure that there is adequate consideration and accountability for the decision-making process.
    f. Wherever possible, the appropriate public authorities will be asked to comment on the impact of any proposed exclusion on the child's broader welfare.
    g. The sharing of data with Members is controlled by a strict data integrity agreement and if the agreement is breached procedures are in place to identify the guilty party [security seeding] and act accordingly with sanctions available.
    h. Children's data will only be retained for 6 months [normally 12].

98. The BCRP processes personal data under the lawful basis of legitimate interest under GDPR Article 6 (1) (f).

99. The justification for the decision is that the interests of our Members outweigh any impact on individuals and the BCRP employs sufficient safeguards to protect the interests of data subjects.

Next Review: October 2022

100. **Data Protection Impact Assessment** [detailed]

Data Protection Issue	Assessment of Risk	Mitigation Measures	Conclusion
<u>Purpose Specification</u> Is the data to be collected to be used only for a specified purpose? Will the data collected be used for anything other than the specified purpose?	The data is used for purposes other than an exclusion notice scheme. Once shared with Members the data could be used maliciously to embarrass or harass data subjects.	Data shared with Members is the minimum required to enforce the exclusion notice scheme. Data sharing with Members is subject to a strict data integrity agreement to which members must recertify every 13 weeks. Measures are in place to identify the source of any breached data [offender photographs are security seeded with a unique code for each Member]. Members do not receive automatic access to data. Measures are in place to verify an applicant's bona fides. Sanctions are in place to punish any deliberate breach. Data is retained only for as long as it is required to fulfil the purpose of the exclusion notice scheme.	**Risk not fully mitigated but accepted.** There are safeguards in place to prevent data being used for any other purpose but it could still happen.
<u>Information quality and accuracy</u> What processes are in place for ensuring information quality i.e. that			**Risk sufficiently mitigated.**

the information is relevant, reliable, accurate, actionable? Is there a policy or procedure in place to correct data that has already been shared with partners, or to notify partners about updates?	Second or third hand data or hearsay could be processed and used to issue an exclusion notice. Incorrect information could be available to partners after is has been found to be inaccurate. Poor quality information may lead to inappropriate decisions that have a negative impact on the individuals concerned.	The confidence test applied to all reports from Members will not allow inaccurate or doubtful data to be processed. Information is centrally controlled by the database administrators. When deleted or corrected old versions are automatically deleted.	Only data from a known source and of proven accuracy will be processed.
<u>Legal basis for data processing data</u> **Legitimate interest** Are individuals able to appreciate the most likely consequences (including negative) of their data being collected? Does the processing involve complex technologies?	The individuals may not know that their data is being processed or the consequences of the processing [sharing, exclusions etc] at the time of processing. Individuals may not understand the nature of the processing even when informed. Data may be lost or intercepted before or during processing.	They will be informed about the data being processed via a 'warning letter' and a privacy notice within five working days of receipt of their data. As required by Recital 39, warning letters have a reading age of 10 years and are simple to understand. The BCRP website has a FAQ section devoted to exclusion notices and another devoted to data protection offering 'bite sized' answers to common questions.	**Risk not fully mitigated but accepted.** Individuals will probably object to their data being processed.

How do individuals object to their information to be processed? Is the individual explicitly informed about how their information can be used or shared with other agencies? Is there an alternative legal basis for processing?	Individuals may be wrongly identified and their data processed without legitimacy. Individuals may be shocked or upset that their data is being shared with members and other agencies.	Data processing employs end-to-end encryption. Email communication including personal data is sent via CJSM accounts. The warning letter includes details of an appeal procedure. The individual is informed about data sharing in the privacy notice and the number of agencies with which data can be shared is strictly on a need-to-know basis and subject to a data sharing agreement. If it is not possible to obtain informed consent or process personal data on an alternative legal basis.	
Are individuals provided with the possibility to access and correct their personal information? Can they request the deletion of some or all of their personal information?	Some individuals may complain about how difficult it is to understand the nature of the processing and if necessary, amend (or delete) their personal data. Individuals may complain to the ICO or the media and/or seek a legal remedy.	Warning letters detail the data we process and they have a reading age of 10 years and are simple to understand. The BCRP website has a FAQ section devoted to exclusion notices and another devoted to data protection offering 'bite sized' answers to common questions. How to complain to the ICO is included in the warning letter and privacy notice. The BCRP has full D&O insurance cover to respond to any legal challenge.	**Risk sufficiently mitigated.** All steps are taken to inform the data subject of the nature of the data we are processing in a straightforward and timely manner.

Is it necessary to restrict access to data? If so, are these restrictions adequately circumscribed and explained?	Individuals may want a full list of all data the BCRP holds and the source of the data. Will processing and sharing result in unwarranted harm to the data subject?	There are no restrictions placed on access to their data either in the initial privacy statement or in subsequent SARs. It will not result in unwarranted harm. Using the Oxford English Dictionary definition of 'unwarranted' [lacking a good reason; unnecessary] it will not result in unwarranted distress although it may result in some distress because it restricts the individual's liberty to enter some retail premises.	
<u>Appropriate security measures</u> What personal information is to be collected? Could disclosure of this information put the person in danger (for example information relating to ethnicity, religion, sexual orientation, political views, trade union membership, etc)? Is there a risk of information being stolen / lost / altered / rendered unavailable / system hacked / organisation subject to surveillance? What preventative measures are in place? Does the processing involve external organisations or third parties? Does	External hackers and rogue employees may seek to exploit personal data. The BCRP may not have strong controls for access to its database. Weak passwords may not protect data. The security controls of the BCRP's systems are breached and personal data is compromised. The BCRP may not know when the personal data it holds is compromised.	No sensitive personal data is processed and only name, date of birth, a photograph and a two or three word description of the offences for which the individual is known are shared with members. Alleged offences against our members are processed together with bail and/or CPN and CBO conditions but this does not constitute a comprehensive register. The BCRP secure Cloud based databases which are certified to the Cyber Essential Standard. The Data Processors for the BCRP maintain their own certified and comprehensive Information Security Management Systems [ISMS] to the ISO27001:2013 standard and all its Cloud-	**Risk sufficiently mitigated.** The security measures put in place are sufficient to adequately protect data.

this increase the risk of surveillance / disclosure by the processor (whether lawfully or not) / hacking / data theft / availability? Is information limited to others on a "need to know" basis? How is this implemented in practice? Is training given to all staff on good data protection and information security practices? Are e-mails encrypted? What action will be taken if there is a data breach? Are individuals informed if their personal data is lost, stolen or other compromised? Will any other organisations be informed?	Individuals may be embarrassed or upset that their personal data is not secure.	service providers are also certified to the same standard. Data is only available to Members and other parties with which we have a data sharing agreement and it is limited to name, date of birth, a photograph and a two or three word description of offences against out members for which the data subject is known. Data protection training is given at induction of new staff and annually thereafter. Emails including personal data are sent via the CJSM network. In the event of a breach the individual will be informed and, after assessment of the severity of the breach, it may be reported to the ICO. The owner/source of the data will also be informed.	

Source of risk and nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Overall risk before mitigation**	**Mitigation**	**Risk after mitigation**
Incorrect data is processed leading to incorrect exclusion.	Probable	Significant	High	Application of the confidence test before processing. Warning letter giving individual an appeal procedure.	Low
Malicious submission of false incident report about an individual.	Possible	Significant	High	Application of the confidence test before processing.	Low
Storage of personal data on laptops leading to loss of personal data.	Possible	Significant	High	No data is stored on any device. Data is stored in secure Cloud-based databases.	Low
Interception of data contained in emails.	Possible	Minimal	Medium	Personal data in emails is limited to secure CJSM server.	Low

Illegitimate access to personal data by third parties. Corporate risk of a data breach as defined by ICO.	Probable	Significant	High	Minimal data is available on the Member-facing databases. Personal data available to Members is limited to name, date of birth, photo and brief two or three word description of offences against members for which they are known. Access to the Member-facing databases is password protected and access for Members is assessed and granted via an administrator. Procedures in place to identity members seeking access to the databases. Members sign a data integrity agreement prohibiting transfer of data to third parties. Member access is withdrawn periodically and they are obliged to recertify adherence to data integrity agreement every 13 weeks. Sanctions are in place for breach of the BCRP data integrity agreement which will deter members from breaching data rules.	Medium

Data Security Breach Management Plan

Introduction

101. The BCRP is committed to ensuring that all personal data we process is managed appropriately and in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) [collectively referred to as "data protection legislation"].

102. As the BCRP processes personal data it is committed to ensuring all unauthorised or unlawful processing, loss, destruction of or damage to data (personal data breaches) are swiftly identified and reported internally and, where appropriate to the Information Commissioner's Office and the data subjects affected.

103. Negligent or malicious non-compliance with this policy may result in disciplinary action. As well as defining BCRP's policy, this procedure lays out the actions, once a breach has occurred.

Scope

104. This policy and procedure applies to all users of BCRP's information, data and information systems and specifically our intelligence database[s]. It applies not only to staff and Members but also, where applicable, contractors, work experience personnel, service providers, consultants and anyone else engaged to work in the organisation and encompasses data, information and software systems.

105. This policy should be read in conjunction with other useful documents, for example:

    a. **ICO Information Security Guide**
    b. **ICO Guidance on Personal Data Breaches**

Responsibilities

106. The Data Controller has overall responsibility for deciding whether to report personal data breaches to the ICO and/or to affected individuals and has overall responsibility for monitoring compliance with this procedure.

107. Although the Data Controller has overall responsibility for monitoring compliance with this procedure, they will delegate the day-to-day management of breach prevention to the crime manager[s].

108. Local BCRP are responsible for ensuring that all members of staff are aware of their responsibilities to report incidents and provide all appropriate information and support relevant to an incident and for continuing incident management and mitigation.

109. All members of staff are responsible for immediately reporting any incident or breach affecting personal data to their line manager in the first instance. Managers are responsible for reporting breaches to the DPO.

110. Personal data about offenders held on paper should be avoided at all costs. Personal data transmitted in emails must use a secure cjsm account.

Types of Breach

111. A number of factors could cause data protection breaches. The following is a list of examples but it is not exhaustive and there may be others which will need to be considered at the time of the breach:

    a. loss or theft of data.
    b. loss or theft of equipment on which data is stored.

c. inappropriate access controls allowing unauthorised use.
d. equipment failure.
e. human error in dealing with personal information.
f. unforeseen circumstances such as fire or flood.
g. hacking attack on the BCRP's ICT systems.
h. 'Blagging' offences where information is obtained by deceiving the organisation who holds it.
i. unauthorised access into secure areas.

Notification of Breaches Once Discovered

112. Instances of the loss of personal data by the BCRP have never occurred at the time of writing, however, the reputational damage and the potential impacts on individuals of the loss of personal information means we need to take swift action in the event of a loss.

113. The person who discovers a breach must inform their line manager immediately. Managers will then inform the DPO. Any breach discovered outside of normal working hours should be reported as soon as is practicable during the next working day. However any serious breaches that could cause serious adverse effect must be reported as a matter of urgency as soon as discovered.

114. The DPO will then decide whether to involve other members of staff, the Data Controller and the ICO.

Assessing the Risk

115. The DPO will carry out the initial assessment of the breach on the day it is reported and consider whether the event meets the GDPR definition of a personal data breach.

116. During this initial assessment, a risk assessment of the impact on the rights and freedoms of the affected data subjects will be undertaken and completed within 72 hours of the breach being first reported.

117. This will consider the risks to the affected individuals arising from the personal data breach including adverse impact on their:

a. Privacy.
b. Personal financial interests.
c. Other material damages.
d. Health and safety.
e. Emotional wellbeing.
f. Other non-material damages.

118. In considering the breach the following factors will be considered (not an exhaustive list):

a. The type of breach.
b. The nature, volume and sensitivity of the personal data breached.
c. How easy it is to identify individuals.
d. The potential consequences for individuals.
e. Any special category characteristics of the data subject.

119. Some data security breaches will not lead to risks beyond possible inconvenience, for example if a laptop is irreparably damaged or lost because, in line with the Information Security Policy, no personal data is stored on the device. There will be a monetary cost to the Company by the loss of the device but not a security breach.

120. Whilst these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of offender data.

121. The following may also be taken into account:

a. what type of data is involved?
b. how sensitive is it? Is it sensitive personal details as defined by the Article 9 of GDPR or other data types which are sensitive because of what might happen if it is misused?
c. if data has been lost or stolen, are there any protections in place such as encryption [in line with the Information Security Policy, all flash drives must be encrypted]?
d. what has happened to the data?
e. can the data be restored or recreated?
f. how usable is the lost data?
g. if data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relates? If it has been damaged, this poses a different type and level of risk.
h. what could the data tell a third party about the individual?
i. how many individuals' personal data is affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.
j. who are the individuals whose data has been breached? Are they staff, offenders, partners or suppliers?
k. what harm can come to those individuals because of the breach? Are there risks to physical safety or reputation, financial loss, fraudulent use or a combination of these and other aspects of their life?
l. are there wider consequences to consider such as a risk to loss of public confidence in the BCRP?

Reporting Personal Data Breaches to the Affected Individuals

122. As part of the risk, the DPO will consider whether the individual[s] whose information has been breached should be informed. Inform the individual[s] concerned, as suggested by guidance from the Information Commissioner.

123. If the DPO considers the personal data breach a high risk, a report will be provided to the Data Controller and ICO including a recommendation on whether to report the breach to the affected individuals.

124. If the individuals are notified the following will be considered:

a. what is the most appropriate method of communication bearing in mind the security of the medium as well as the urgency of the situation?
b. the notification will include as a minimum, a description of how and when the breach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will also be included.
c. the individuals will be given clear advice on what they should do to protect themselves and what [if anything] the BCRP can do on their behalf.
d. a means of contacting the Data Controller for further information will be provided in addition to any other named individual[s] or a web page or a combination of all of these.

Appointment of Lead Investigator

125. The DPO will, in consultation with others if necessary, decide who the Lead Investigator should be and who needs to be involved and will work with them to manage the breach. The DPO is

responsible for assessing the impact of any breach of the data protection legislation. This can include recommendations to restore data security.

126. The Lead Investigator could be any of the following:

    a. a member of the board.
    b. the DPO.
    c. Chief Executive[s].
    d. a BCRP manager.
    e. a combination of the above.

127. The Lead Investigator/DPO must also consider whether the police need to be informed. This could be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future or if the breached data belongs to the police and has been shared under a DSA. If necessary all staff will be informed to prevent additional breaches.

128. The DPO will maintain a log with the details of all breaches. This will include who the Lead Investigator is, when the breach occurred, who is involved and what action must be taken after the breach.

Investigation Procedure

129. The investigation will commence immediately on receipt of notification. It will be completed urgently and wherever possible within 72 hours of the breach being reported. If necessary, a further review of the causes of the breach and recommendations for future improvements will be carried out once the matter has been resolved.

130. The Lead Investigator should ascertain whose data was involved in the breach, the person or people responsible for the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

131. Breaches will require not just an initial investigation and a decision on the severity and containment of the situation but also a recovery plan including, where necessary, damage limitation. This may involve input from the Data Controller and also the Company's legal advisors[16]. In some cases, contact with external stakeholders or suppliers may be required.

132. The Lead Investigator will establish the questions for interviews and then meet with the participants. This could be (but is not limited to, or necessarily, all of them) witnesses, perpetrators, junior officers and senior managers.

133. Working with the Lead Investigator the DPO will identify if there is a need for expert advice from the Company's legal advisors[12].

134. Issues to be addressed during the investigation will include:

    a. the date when the breach occurred.
    b. the date when the breach was discovered and by whom.
    c. the type of data and the number of records involved.
    d. the sensitivity of the data.
    e. the circumstances of the release
    f. what protection is in place (for example encryption).
    g. what has happened to the data.

[16] Acumen Business Law

h. whether the data could be put to any illegal or inappropriate use.
i. how many people are affected.
j. what group of people has been affected (the public, suppliers, offenders etc).
k. whether there are wider consequences of the breach.

135. The Lead Investigator will keep an electronic record of all activities during the investigation. This could include the actions taken to mitigate the breach and lessons learnt. The reason being that the records may need to be shared if there are actions by the police, Information Commissioner or legal proceedings.

136. If the DPO is not also the Lead Investigator, the Data Controller will assist the Lead Investigator, where necessary. This could include informing the Information Commissioner's Office, calculating the severity of the incident, informing the wider board of directors, collating reports and suggesting actions to be taken.

137. If systemic or on-going problems are identified, an action plan will be drawn up to correct the issues identified and the wider board of directors will be informed. If the breach warrants a disciplinary investigation (for example due to negligence), the Data Controller will make the final decision on sanctions against staff.

138. The Lead Investigator should produce a report for the Data Controller bearing in mind that it may also be shared with the ICO. The report must address the following:

a. establish the facts (including those that may be disputed.)
b. include a chronology of events including the containment, recovery and how the breach has been investigated.
c. a risk analysis.
d. a commentary of the weight of evidence
e. action to minimise/mitigate effect on individuals involved including whether the victims have been informed.
f. whether any other regulatory body and been informed and their response.
g. recommendations to reduce the chance of the same breach happening again.

Containment

139. At the same time as an investigation is happening, containment and [if necessary] recovery will also happen. The Lead Investigator must ascertain whether the breach is still occurring. If so, it must be stopped immediately to minimise the effect of the breach. This will involve liaison with appropriate staff; examples might be the Chief Executive[s] authorising the shutdown of the Company's database system[s] or stopping the delivery of non-secure emails.

Reporting Personal Data Breaches to the Information Commissioner's Office

140. The GDPR places a duty on all organisations to report certain types of data breach to the Information Commissioner's Office. In the case of a personal data breach, the BCRP shall without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach, notify the ICO, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual. A reason for the delay, if notification is not within 72 hours, is required along with the notification.

141. The GDPR states that a personal data breach must be reported to the ICO if the breach is likely to result in a risk to the rights and freedoms of the individuals concerned. By this, it means discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. It also requires that this be on a case-by-case basis. There is no need to notify the ICO if there is not a risk to persons' rights and freedoms however, if the breach is

of data contained in the BCRP's Member-accessible database system[s], it is very *unlikely* that the breach will not have to be reported.

142. After carrying out a full assessment of the risk, the decision as to whether or not to inform the ICO would normally rest with the Data Controller. If the decision is to notify the ICO and the DPO will act as liaison with the ICO.

Review

143. A policy review will take place after a serious breach or after legislative changes, important changes in case law or guidance.

Appendix A

PERSONAL DATA BREACHES

Copy-and-paste the following form to create a new form for each reported Breach; be sure to document all communications with your Data Processor, ICO and, where necessary, any relevant Data Subjects.

1	Report type. *delete as appropriate*	*Initial Report* *Follow up Report* *If follow up: ICO Case Ref.*	***Notes***
2	Reason for the report	*I consider this incident meets the threshold.*	*Use ICO toolkit to test.*
3	What happened and how the incident occurred?		*Eg: Malicious attack (internal or external?); accidental (technical security failure); negligence/human error (operation security failure); other (specify).*
4	How did we discover the breach?		
5	If there was a delay in reporting the breach explain why.		*72 hour deadline.*
6	What preventative measure did we have in place?		
7	Was the breach a cyber incident?	Yes No Don't know	*Any event that threatens the security, confidentiality, integrity, or availability of CABQ information assets e.g. Phising attack, DdOS, Ransomware.*
8	Date the breach happened?	Date: Time:	*Notify the relevant Data Processor as soon as you are aware of the Breach*
9	Date we discovered the breach.	Date: Time:	*Notify the ICO within 72 hours of the detection of the Breach (see 5 above).*
10	Date of notification to Data Subjects if necessary.		*Does incident meet the threshold for such communication?*
11	Personal Data Included in the breach.	Racial origin Political opinions. Religious beliefs Trade Union Membership Sex life data. Sexual orientation data Gender reassignment data. Health data. Basic personal identifiers [e.g. name, contact details. photo]. Identification data [e.g. usernames, passwords].	

		Economic & financial data [e.g. credit card numbers, bank account]. Official documents [e.g. driving licence]. Location data [e.g. coordinates]. Genetic or biometric data Criminal convictions. Other.	
12	Number of personal data records involved?		
13	Number of data subjects likely to be affected?		
14	Types of data subjects affected.	Employees Users Subscribers Students Customer Patients Children Vulnerable adults Offenders Other	*Delete as appropriate*
15	Potential consequences of the breach.		
16	Is the personal data breach likely to result in high risk to the subject[s]?	Yes [Give details] No Not yet known	*Delete as appropriate*
17	Had the staff member involved in the breach received data protection training in the last 2 years.	Yes No Don't know	*Delete as appropriate*
18	The actions we have taken as a result of the breach.		
19	Have we told the data subject about the breach?	Yes – it is likely there is a high risk to the subject Yes – it is not likely there is a high risk but we have told them anyway. No – but we are planning to. No – the incident does not meet the threshold for communicating with the data subject[s].	*Delete as appropriate*
20	Have we told, or will we tell, any other organisation about the breach?	Yes [name them] No Don't know	*Does any of the data belong to partners or other agencies?*

21	Organisation submitting this report	
22	Address	
23	Data Controller	
24	ICO Registration	
25	Contact name	
26	Email and phone number	