

Brighton & Hove Business Crime Reduction Partnership [the Scheme]

PERSONAL DATA PROCESSING ON CHILDREN & MINORS ON THE BASIS OF LEGITIMATE INTEREST

1. This document describes the way that personal data is processed and secured by the Scheme.
2. **Contact details**
Brighton & Hove BCRP Ltd
PO Box 5398
Brighton BN50 8GQ
Email address: noreply@bcrpbrighton.com
Tel: 01273 733393
3. The Scheme's Data Controller is responsible for ensuring its compliance with current Data Protection law and can be contacted at the above address, email address or telephone number. The Scheme is registered with the Information Commissioners Office as a Business Crime Reduction Partnership.
4. **Background**
The General Data Protection Regulation [GDPR] does not ban an organisation from relying on legitimate interests as a lawful basis if it is 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.'*¹
5. 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.
6. 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, GDPR does not prescribe the age at which a person is considered to be a child.
7. 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, once again, 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."
8. 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'.

¹ Article 6 (1)(f)

9. 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 and in England & Wales 10 years of age is the lower threshold of criminal culpability.
10. 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.
11. 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.
12. 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 14²". 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.
13. It is the belief of the BCRP that the age of 10, or even 12, is too young to fully understand criminal culpability.
14. **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 has set a minimum age of 14 for the processing of offender data.**
15. **Legitimate Interest Assessment**
The basis for the processing of children's data will be subject to a Legitimate Interest Assessment [see Appendix 1]. The BCRP is aware that ideally a data protection subject matter expert should carry out an LIA. However, given the small size of the BCRP and limited financial resources this is not possible but an individual with appropriate seniority will be given responsibility to ensure that there is adequate consideration and accountability for the decision-making process.

Categories and types of personal data processed

16. **Offender's name and facial image [a picture made using a camera] and any relevant information about the nature of his/her anti-social activities in connection with our Members' interests;** the purpose of this processing is to enable Members to identify Offenders in order to submit reports about them, to include them in a list or gallery of excluded persons (if appropriate and in line with the Scheme's Rules & Protocols), and to provide information about them which may be necessary to protect the personal safety of Members and their staff, customers etc. This data may be shared among Members;
17. **Offenders' postal and email addresses, telephone number(s) and other contact details;** the purpose of this processing is to enable the Scheme to communicate with Offenders from time to time, for example to send confirmation of exclusions, rules of the exclusion scheme, or confirmation that exclusions have expired. Such data will not be shared with Members.

² The minimum age is 12 in the Netherlands, 13 in France, 14 in Germany, 15 in Sweden and Italy, 16 in Spain and 18 in Belgium

18. **Information and evidence about 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. Details of such data will not be shared with Members but rather a one or two word description of the general offence for which the offender is known. 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

19. 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. The BCRP's processing of special category data is limited *per se* in any event but especially so in the case of children who are afforded special protection[s] under GDPR
20. The lawful basis for the processing of special category data is Article 6. 1(e) - processing is necessary for the performance of a task carried out in the public interest.
21. Such processing [necessary for reasons of substantial public interest, on the basis of Union or Member State law] 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)].

22. The following table outlines what special category data will be processed, with whom it will be shared and the reason for distribution:

Category	Processed?	May be shared with?	Justification
Race	Will not be processed	Will not be shared	
Ethnic origin	May be processed	Members. Other accredited BCRPs in Sussex. National Business Crime Solution.	For the purposes of assisting BCRP Members to identify excluded individuals
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 taken with a camera and not subject to any specific technical processing may be processed ³ . No other biometric data will be processed.	Members. Other accredited BCRPs in Sussex. National Business Crime Solution.	For the purposes of assisting BCRP Members to identify excluded individuals
Health data	Will not be processed	Will not be shared	
Sex life	May be processed	Will not be shared	To protect an individual's vital interests when deemed at risk e.g. potential for Child Sexual Exploitation. There will be no additional processing other than implicit references from other data sources where necessary. This information will be redacted where possible from other reports.
Sexual orientation	May be processed	Will not be shared	To protect an individual's vital interests when deemed at risk e.g. potential for Child Sexual Exploitation. There will be no additional processing other than implicit references from other data sources where necessary. This information will be redacted where possible from other reports.

³ A photograph was deemed to be biometric data in the Judicial Review M vs Chief Constable of Sussex Police

Sources of personal data

23. **Offenders** themselves who may voluntarily offer information;
24. **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;
25. **Other business crime reduction partnerships** or similar accredited private sector agencies with which we have a data sharing agreement
26. **Police or other public agencies** may provide Offenders' personal data under a formal Data Sharing Agreement
27. **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.

Data Retention Period

28. When an Offender is reported by a Member 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. If the data fails the confidence it will be irrevocably destroyed immediately without any further processing. If it passes the confidence test the Offender's name, date of birth and facial image may be shared among Members for a maximum of 12 months. If no further report is submitted during that period, the Offender's data will be withdrawn from Members at the expiry of that period. It may be retained for a further maximum of 6 months in the Scheme's database. During this latter period it will not be shared with members and can only be accessed by the Data Controller and authorised personnel. At the end of this latter period data must be irrevocably deleted unless further reports of criminal and/or anti-social behaviour involving a threat or damage to any Member's property, staff or customers are reported to the BCRP [see paragraph 23 below].
29. If during the 12 months when an Offender's data is circulated among Members he/she is reported for another incident involving a threat or damage to any Member's property, staff or customers, his/her name and facial image may be circulated among Members for a further maximum of 12 months from the date of the second report. Additionally, the Offender may be excluded from all the properties of all Members for 12 months, and this fact will be shared with Members. If no further report is submitted by a Member during that period, the Offender's data will be withdrawn from Members at the expiry of that period. It will be retained for a further maximum of 6 months in the Scheme's database (which can only be accessed by the Data Controller and authorised personnel) after which it will be irrevocably deleted.
30. A limited range of personal data may also be transmitted via the radio network operating in the city. All radio transmissions will be recorded on the BCRP's Safety Net radio management system and will be stored for a period of 6 months after which they will be erased. This data will only be shared with law enforcement agencies to support the investigation of a crime.

Balance of interests

31. Using the minimum age of 14 is deemed to be proportionate when balanced against the interests of our Members 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.

32. The BCRP is aware that, for children of this age group [and up to 17] the free association with groups of their peers in the city centre is a significant element of their socialisation which will be disrupted by being subject to an exclusion notice. However, we do not consider that the impact of any exclusion notice will be damaging to their ability to socialise since our members constitute only a small percentage of the total number of the retail outlets in the city and there is no exclusion from public places where young people tend to congregate.
33. However, the default position is not to exclude children [or indeed adults] and every effort will be made to avoid or remediate exclusion by:
- a. Wherever possible taking into account that assessing the degree and level of understanding by the child, rather than merely determining age, is key to ensuring that personal data about children is collected and used fairly. Any mitigating circumstances or characteristics of the individual will be considered prior to action being taken.
 - b. Comment on individual exclusions will be sought from the Youth Offending Service and any other relevant statutory agencies but these agencies will play no direct part in the ultimate decision making process to avoid any adoption of a 'public function'
 - c. Issuing warning letters to the individual's parents/guardians after the first reported incident making it clear, in language that their children will also understand, that the consequences of continued offending will result in exclusion and listing the premises from which they will be excluded [the identity and address of the parent[s] or guardian may be collected for the sole purpose of communicating relevant information about their children].
 - d. Offering 'putting it right' sessions to children who have been reported for the first time and have no previous history of criminal activity.
 - e. Ensuring that cases involving the exclusion of children are given full consideration by the Board of Management and that evidence is verified as being accurate and fair.
 - f. In the event of an exclusion, ensuring that the appeals procedure is drawn to the attention of the parents/guardians.
 - g. Data on offenders under the age of 18 will be stored for 6 months after the expiry of an exclusion notice [12 months for adults].

Data Processors

34. The Scheme employs the services of the following Data Processor(s):
35. **Littoralis Limited**; access the Littoralis Standard Terms & Conditions including our Data Processor Contract with the company [here](#)

Standard Operating Procedures

36. The following Standard Operating Procedures have been defined relating to the processing of personal data by the Scheme and in compliance with current Data Protection law:

Documentation management

37. Every six months the Data Controller 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 *Balance of Interests Statement(s)* and, where relevant, *Information Sharing Agreement(s)* and *Data Processing Agreement(s)*.
38. 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);

39. 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.

Subject Access Requests

40. Within 30 days of an applicant submitting a Subject Access Request to the Data Controller or Board of Management, the Data Controller must confirm its receipt with the applicant;
41. 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;
42. As soon as practical thereafter the Data Controller must:
- a. collect all personal data relating to the applicant, including image(s);
 - b. redact all data identifying any other person from the data;
 - c. provide the relevant personal data to the applicant, in a conventional, readable format;
 - d. provide all documentation demonstrating the Scheme's compliance with Data Protection law;
 - e. inform the applicant of his/her 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. Document the completion of the SAR process

Reporting a Personal Data Breach

43. 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;
44. As soon as possible thereafter, in the case of a data breach which, in the view of the Board of Management, 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.
45. The Data Controller must document each Personal Data Breach in **Appendix A** of this document

46.

Privacy Notices distribution

47. **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. We will use best endeavours to record the service of the Privacy Notice and retain record of service;
48. **Where data is not collected directly from the Offender:** as soon as possible thereafter, use best endeavours to serve a Privacy Notice (Offender) [unless the provision of such information proves impossible [GDPR Article 14, para 5(b)] and record the service of the Privacy Notice and retain record of service;
49. In any case to display Privacy Notice (Offenders) on the Scheme's website where it is publicly available to maximise likelihood and possibility of access by Offender accompanied by a Frequently Asked Questions [FAQs] page on both Exclusion Notices and Data Protection.

The Children's Act 2004

50. The Act states that voluntary organisations and private sector providers can play an important role in safeguarding children. The BCRP will aim to work effectively with the statutory agencies and will set out clearly the processes for sharing information with those agencies as appropriate. BCRP staff will be aware of their responsibilities for safeguarding and promoting the welfare of children, how they should respond to child

protection concerns and how to make referrals to local authority children's social care, Youth Offending Team [YOS] and/or the police as necessary.

Appendix 1

Legitimate Interest Assessment [LIA] [Children]

1	Legitimate Interest Test	
A	What is the purpose of the processing operation	<p>1. To protect the property of our Members from harm and their 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.</p> <p>To monitor the activity of those children in danger of exclusion from our Member's premises and entry into the criminal justice system and, wherever possible, intervene to prevent the same.</p>
B	Is the processing necessary to meet one or more specific organisational objectives?	Yes. The Scheme processes Offenders' personal data for the management of its Exclusion Scheme on behalf of its Members, to inform Members of an offender's modus operandi, to collate intelligence on criminal activity within the area of the Scheme's operation and to contribute to legal proceedings against Offenders where appropriate.
C	Is the processing necessary to meet one or more specific objectives of any Third Party?	Yes. The objectives of our Members
D	Does the GDPR, ePrivacy Regulation or other national legislation specifically identify the processing activity as being a legitimate activity, subject to the completion of a balancing test and positive outcome?	<p>Yes. Article 23 of the GDPR allows for derogations and the Data Protection Act 2018 permits the processing of data without consent on the basis of Legitimate Interest for</p> <ul style="list-style-type: none"> • the 'prevention, investigation, detection or prosecution of criminal offences' and also • the 'protection of the individual, or the rights and freedoms of others'.
2	Necessity Test	
A	Why is the processing activity important to the Controller?	<p>It identifies threats to the property of our Members or their staff and customers and seeks to reduce or remove the threat through targeted actions against offenders. Our Members have vested in the BCRP certain authorities to carry out actions on their behalf.</p> <p>It also permits interventions at an early stage to prevent children from entering the criminal justice system and/or being excluded from our Member's premises.</p>
B	Why is the processing activity important to other parties the data may be disclosed to?	It is important to our Members because it informs and identifies individuals against whom the BCRP has taken action so that they can be prevented from entering their premises. It also informs them of children who are in danger of exclusion so that they can intervene to prevent exclusion.
C	Is there another way of achieving the objective?	No

3	Balancing Test	
A	Would the individual expect the processing activity to take place?	It depends upon the nature of any offences committed. If police are involved in such incidents then they would.
B	Does the processing add value to a product or service that the individual uses?	No.
C	Is the processing likely to negatively impact the individual's rights?	No. Not on their rights under GDPR. Their right to enter our Member's premises is tacit and can be withdrawn at any time under Common Law.
D	Is the processing likely to result in unwarranted harm or distress to the individual?	No. It will not result in unwarranted harm. Using the Oxford English Dictionary definition of 'unwarranted' [<i>lacking a good reason; unnecessary</i>] 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.
E	Would there be a prejudice to Data Controller if processing does not happen?	Yes. The BCRP's Members expect the data controller to act in a manner that protects their property and hence it would result in prejudice if the processing was not carried out.
F	Would there be a prejudice to the Third Party if processing does not happen?	Yes. To the BCRP Members against whom offences are committed.
G	Is the processing in the interests of the individual whose personal data it relates to?	Under some circumstances. If it prevents children from entering the criminal justice system via early intervention by the BCRP [and other agencies] it is of benefit to the individual.
H	Are the legitimate interests of the individual aligned with the party looking to rely on their legitimate interests for the processing?	Under some circumstances. If it prevents children from entering the criminal justice system via early intervention by the BCRP [and other agencies] it is of benefit to the individual.
I	What is the connection between the individual and the organisation?	None.
J	What is the nature of the data to be processed? Does data of this nature have any special protections under GDPR?	Name. Date of birth. Photographic image. Address. Offences against BCRP Members. The processing of children's data enjoys special protection under the GDPR but UK derogations allow the processing of such data for the purposes of the prevention of crime and disorder.
K	Is there a two-way relationship in place between the organisation and the individual whose personal information is going to be processed? If so how close is that relationship?	Yes. There will be a periodic two-way relationship for the duration that the data is held or an exclusion notice is in force.

L	Would the processing limit or undermine the rights of individuals?	It would not affect the rights of the individual under GDPR but it would limit his/her tacit invitation to enter certain private premises in the city of Brighton
M	Has the personal information been obtained directly from the individual, or obtained indirectly?	Directly Indirectly Both
N	Is there any imbalance in who holds the power between the organisation and the individual?	Yes. But the imbalance is mitigated by those measures listed in paragraph 14
O	Is it likely that the individual may expect their information to be used for this purpose?	Yes. Wherever possible, they [or their parent/guardian] will be informed at the outset.
P	Could the processing be considered intrusive or inappropriate? In particular, could it be perceived as such by the individual or in the context of the relationship?	It may be considered intrusive or inappropriate by the individual but, given the nature of the incidents that result in data processing, it would not be perceived as such by any reasonable assessment by an uninterested third party.
Q	Is a fair processing notice provided to the individual, if so, how? Are they sufficiently clear and up front regarding the purposes of the processing?	Yes. By post where an address is known immediately upon receipt of any data from any source. It is sent to the parent/guardian but is written in language that children can understand.
R	Can the individual, whose data is being processed, control the processing activity or object to it easily?	To an extent they can control it via the appeal procedure. They can also object to it. Procedures for doing so are included in the initial letter and straightforward access to the appropriate appeal process is via the BCRP website.
S	Can the scope of the processing be modified to reduce/mitigate any underlying privacy risks or harms?	Yes. See below
T	Safeguards & compensating controls	Information of offences will be shared with the parent/guardian immediately upon receipt of the first incident report in language that the child will also be able to understand. Information will also be shared with the statutory agencies e.g. Adolescent Services, Youth Offending Service etc. Their opinion of the effect of data processing on the wellbeing of the child will be seriously considered during the decision making process. Until the threshold for exclusion is reached information will not be shared with Members.

		<p>Upon reaching the threshold, the Board of Management [BOM] will give consideration to whether exclusion is required/appropriate taking into account any mitigating circumstances or information provided by the Youth Offending Service. The BOM will also consider whether exclusion from all venues is required/appropriate; if not, information will only be shared with the relevant members.</p> <p>Data will only be retained for 6 months after the expiry of any exclusion notice [normally 12 months].</p> <p>All members sign a binding data integrity agreement which prevents them from sharing information with third parties who are not Members of the BCRP. If the data integrity agreement is breached, procedures are in place to identify the guilty party and act accordingly.</p> <p>Particular attention will be drawn to the appeals process when communicating with the individual.</p>
U	Outcome of assessment	<p>It is the conclusion of the BCRP that the Legitimate Interest basis for the processing of personal information without the consent of the individual is valid.</p> <p>2. The right of our Members to protect their property from harm and their staff and customers from crime and anti-social behaviour and to exclude from their premises any individuals, including children, 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 is greater than the rights of the individual to privacy.</p> <p>3. Sufficient safeguards are put in place to protect the privacy of the individual and sufficient safeguards can be employed to assess the effect of data processing and/or exclusion on the holistic wellbeing of the child. If it is deemed that the wellbeing of the child would be adversely affected no data processing and/or sharing will be employed.</p>
	Signed by	
	Date	