Information Sharing Agreement

May 2023

PART A. The parties' details

Name of party	NOTTINGHAM CITY COUNCIL ("THE **CITY**)
Party's address	LOXLEY HOUSE STATION STREET, NOTTINHAM NG2

Name of party	NOTTINGHAMSHIRE POLICE ("THE POLICE")
Party's address	SHERWOOD LODGE, ARNOLD, NOTTINGHAMSHIRE ENGLAND, NG5 8PP

Name of party	NHS Nottingham and Nottinghamshire ICB
Party's address	SIR JOHN ROBINSON HOUSE, SIR JOHN ROBINSON WAY ARNOLD, NOTTINGHAM, NG5 6DA

Name of party	NOTTINGHAMSHIRE FIRE & RESCUE
Party's address	JOINT HEADQUARTERS, SHERWOOD LODGE, ARNOLD, NOTTINGHAM, NG5 8PP

Name of party	NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST
Party's address	QMC CAMPUS- Derby Road Nottingham NG7 2UH

Name of party	NOTTINGHAMSHIRE HEALTHCARE NHS FOUNDATION TRUST
Party's address	Duncan Macmillan House, Porchester Road, Nottingham, NG3 6AA

Name of party	NOTTINGHAM CITYCARE
Party's address	Aspect House, Aspect Business Park, Bennerley Road, Bulwell, Nottingham, NG6 8WR

Name of party	DEPARTMENT FOR WORK AND PENSIONS
Party's address	

Name of party	EAST MIDLANDS AMBULANCE SERVICE
Party's address	Trust HQ, 1 Horizon Place, Mellors Way, Nottingham NG8 6PY

Name of party	NOTTINGHAM PROBATION OFFICE
Party's address	9 Castle Quay, Nottingham, Nottinghamshire, NG7 1FW

Name of party	HMP NOTTINGHAM
Party's address	Perry Road, Sherwood, Nottingham, NG5 3AG

Name of party	ALL ADDITIONAL PARTIES AS SET OUT IN THE DETAILS OF PARTIES (ANNEX TO PART A WITH SIGNATURES)

PART B. TERMS

1. Definitions & Interpretation

1.1 In this Information Sharing Agreement (ISA), unless the context requires otherwise, the following terms shall have the following meanings:

"Criminal Conviction Data"	has the meaning given in UK GDPR Art 10, DPA 2018 s.10 and Schedule 1;
"Data Controller"	has the meaning given in the Data Protection Act 2018 and the UK GDPR;
"Data Protection Legislation"	the Data Protection Act 2018, the UK General Data Protection Regulation, the Regulation of Investigatory Powers Act 2000,The Investigatory Powers Act 2016, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699, as amended by Privacy and Electronic Communications (EC Directive) Regulations 2003/2426), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner's Office;

"Data Subject"	has the meaning given in the Data Protection Act 2018 and the UK GDPR;
"DPA"	the Data Protection Act 2018;
"DPIA"	the Data Privacy Impact Assessment referred to in clause 8.1;
"ISA"	this information sharing agreement comprising Parts A (The parties' details), B (Terms)) and C (Information Sharing Annexes);
"**Information Sharing Annex"**	means an information sharing annex in the form of a template at Part C to this ISA which details the information sharing activities and the process for sharing information between the Parties;
"Joint Controllers"	under the UK GDPR, Part 1 of the DPA and Part 3 of the DPA means where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers;
"Law Enforcement Purposes"	under Part 3 of the DPA, the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
"Parties"	means the organisations set out at Part A ('The parties' details)
"Personal Data"	has the meaning given in the Data Protection Act 2018 and the UK GDPR;
"Shared Information"	the information shared in accordance with this ISA and detailed under heading 2 (What information is being shared) of an Information Sharing Annex in Part C to this ISA;
"Special Categories of Personal Data"	means the categories of personal data referred to the Data Protection Act 2018 and in Article 9(1) of the UK GDPR;
"Sensitive processing"	processing for Law Enforcement Purposes that involves (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation

"Purpose"	the purpose for which the Shared Information will be shared in accordance with this ISA and set out under heading 1 (Why is the information being shared?) of the relevant Information Sharing Annex in Part C to this ISA.
"UK GDPR"	UK General Data Protection Regulation (EU General Data Protection Regulation 2016/679) as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and any equivalent legislation amending or replacing the UK GDPR.
"Working Day"	means a day other than a Saturday, Sunday or public holiday in England.

1.2 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

1.3 Clause, schedule and paragraph headings shall not affect the interpretation of this ISA.

1.4 A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

2. Introduction

2.1. Section 42 of the Care Act 2014 places a statutory duty on all local authorities to make enquiries and take decisions whenever there is reasonable cause to suspect that any adult who needs care and support and who is at risk of or experiencing abuse or neglect is unable to protect themselves against such a risk as a result of their needs. To assist in the discharge of this statutory duty, under s. 43 of the Care Act 2014 each local authority is required to set up a Safeguarding Adults Board (SAB) to coordinate local work to safeguard adults who need care and support.

2.2. The Nottingham City Safeguarding Adults Board (NCSAB) exists to fulfil the above duties to safeguard adults at risk in Nottingham from harm and abuse by effectively working together. Members of the NCSAB are representatives of organisations with a statutory responsibility for or interest in safeguarding of adults or are individuals who provide expert opinion or have a specialist area of relevant knowledge.

2.3. Section 44 of the Care Act 2014 requires the SAB to arrange a Safeguarding Adults Review (SAR) whenever an adult at risk of abuse dies or has experienced serious neglect or abuse, and there is concern that the partner agencies could have worked more effectively to protect them. The purpose of a SAR is to determine what relevant agencies and individuals involved could have done differently that could have prevented harm or a death from taking place, and to ensure that the lessons learnt from the review are applied to future cases, with a view to improving safeguarding practice across the SAB partnership.

2.4. The NCSAB Safeguarding Adults Review Sub-Group exists to commission SARs and provide assurances to NCSAB on the procedures, conduct and actions taken following the reviews. Members are drawn from organisations that are represented on NCSAB.

2.5. Commissioning and completion of SARs within Nottingham City requires sharing of Personal Data including Special Categories of Personal Data between organisations that are represented on the NCSAB and the Review Sub-Group.

2.6. This Information Sharing Agreement ("**ISA**") sets out the arrangements for sharing information between the Parties to, amongst other things, demonstrate compliance with the Data Protection Legislation. It consists of the Parties to the ISA as identified in Part A, the Terms in this Part B, and the completed Information Sharing Annex in Part C.

2.7. In the event that a Party withdraws from the ISA (in accordance with clause 9.1) or a new party joins the ISA, an amended and updated version of this ISA must be drafted as soon as practicable and circulated to all Parties for signature and dating.

2.8. Electronic exchange - All information transmitted across public networks within the UK or across any networks overseas must sent by secure email which meets UK central government's connection standards or be encrypted using appropriate software (e.g. Microsoft 365, Egress Switch, Cryptshare, etc.).

- Passwords must be sent separately to the information exchanged and must provide the correct level of security taking all factors into account, including the nature of the data being shared. Passwords must be changed regularly, and the

Parties respective password arrangements will include provisions to avoid the use of weak or predictable passwords.

- Personal exchange of materials for meetings - Information may be hand delivered or taken in hard copy providing it securely contained within a blue locked bag or similar locked bag or container.

3. Purpose of the information sharing

The information is being shared for the purpose set out under the 'Why is the information is being shared?' heading of the Information Sharing Annex in Part C.

4. Information to be shared

The information that may be shared between the Parties under this ISA is listed under the 'What information is being shared?' heading of the Information Sharing Annex in Part C.

5. Legal Basis for sharing

5.1. The lawful basis of processing and information sharing under this ISA is set out in clauses 5.2 and 5.3 with any additional lawful bases detailed under the 'What are the additional legal bases for sharing the information?' heading of the Information Sharing Annex in Part C.

5.2. The Parties are processing Personal Data on the lawful basis of public task, specifically the task of commissioning and completion of Safeguarding Adult Reviews as underpinned by a statutory requirement in the Care Act 2014. Public task is established as a lawful basis for processing in Article 6(1)(e) of UK GDPR ("processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller") and Section 8 of Part 2 Chapter 2 of the Data Protection Act 2018 ("Lawfulness of processing: public interest").

5.3. To the extent that the Shared Information includes Special Categories of Personal Data, the Parties will process that data on the basis of an exception in Article 9(2)(h) of UK GDPR ("the provision of health or social care or treatment or the management of health or social care systems and services") as supplemented by Schedule 1 Part 1(2) in the Data Protection Act 2018 ("health or social care purposes"), and in some circumstances on the basis of an exception in Article 9(2)(g) of UK GDPR ("substantial public interest") where the substantial public interest condition is as set out in Schedule 1 Part 2(18)(1) in the Data Protection Act 2018 ("Safeguarding of children and of individuals at risk").

5.4. To the extent that the information being shared includes any Personal Data, the Parties shall ensure that the Shared Information is processed in accordance with the Data Protection Legislation.

6. Access to data and individuals' rights

6.1. A Party shall contact the other Parties' within 2 (two) Working Days if it receives a subject access request (or purported subject access request) under the Data Protection Act 2018 or a request for access to personal data or information under Article 15 of the UK GDPR and/or a request for information under the Freedom of

Information Act 2000 or the Environmental Information Regulations 2004 in relation to the Shared Information. The other Parties shall provide reasonable cooperation and assistance to the Party in respect of any such request.

6.2. A Party shall notify the other Parties' within 2 (two) Working Days of any request by an individual for rectification or erasure of Shared Information or restriction of processing carried out in respect of the Shared Information in accordance with Article 16 (right to rectification), Article 17(1) (right to erasure) and Article 18 (right of restriction of processing) of the UK GDPR. The other Parties shall provide reasonable cooperation and assistance to the Party in respect of any such request.

6.3. Any request by an individual made in relation to data held for Law Enforcement Purposes will be dealt with by the Party who is the relevant competent authority in respect of the data. The Party that is the relevant competent authority may determine that the request is not subject to Part 3 of the DPA and the request is to be dealt with in accordance with clauses 6.1 and 6.2 above.

6.4. Parties will respond to any notice from the Information Commissioner that imposes requirements to cease or change the way in which data is processed.

6.5. Data Subjects have the right to object to processing. How the Data Subject makes such objections shall be detailed in each Party's Privacy Notice. It is the responsibility of all Parties to produce and maintain their own Privacy Notice.

7. Information governance

7.1. Before starting any information sharing activity detailed in the Information Sharing Annex, each Party will consider whether or not to carry out a Data Privacy Impact Assessment as required under Data Protection Legislation to minimise any data protection risks of the information sharing being contemplated and to establish that the proposed information sharing complies with the Parties' data protection obligations.

7.2. Each Party intending to share data shall be responsible for identifying whether the completion of a Data Privacy Impact Assessment (DPIA) is required, and if it is, will be responsible for completing the DPIA. Each Party will be responsible for considering, adopting, and relying upon the Data Privacy Impact Assessment for their own compliance with the Data Protection Legislation.

7.3. The Shared Information may not be used by the Parties for any other purposes than those set out in the Information Sharing Annex in Part C. If any Party wishes to use the Shared Information for another purpose, that Party will consider the views of all the other Parties as to whether the new purpose is incompatible with the purpose(s) set out under heading 1 of the Information Sharing Annex in Part C, whether they need to complete a new DPIA and the Information Sharing Agreement will be updated and signed by all Parties.

7.4. In accordance with the principle of data minimisation, each Party shall ensure that only information which is necessary to the purpose set out under heading 2 of the Information Sharing Annex will be shared and that only staff for whom it is necessary to access the information for such purpose, have access to the information. No irrelevant or excessive information will be disclosed by one Party to the other Parties.

7.5. Where possible and to the extent that it does not conflict with any of the other provisions set out in this ISA, each Party shall ensure that any Personal Data, Special Categories of Personal Data or Criminal Conviction Data contained within the Shared Information is anonymised or pseudonymised.

7.6. In accordance with its own data protection policy, each Party shall implement appropriate technical and organisational measures to maintain the quality and integrity of the Shared Information held by it, having regard to any specific requirements set out under the heading 'Additional Information' in the Information Sharing Annex in Part C.

7.7. Parties will have procedures in place to report misuse, loss, destruction, damage, or unauthorised access, suspected or otherwise, of information. The Party originally supplying the information must be notified of any breach of confidentiality or incident involving a risk or breach of the security of information shared under this ISA.

7.8. Where possible, the Parties shall ensure that the information is shared using compatible datasets and that any Shared Information is recorded in the same way by each Party.

7.9. Each Party shall ensure that the Shared Information is processed securely and, as a minimum, shall adhere to its own internal information security policy and the 'security requirements' set out in the Information Sharing Annex in Part C.

7.10. Parties must ensure that they have appropriate measures in place to ensure the secure storage of all information disclosed under this ISA as follows:

(a) Information provided must be held in a lockable storage area, office, or cabinet.

(b) Electronic files must be protected against illicit internal use or intrusion by external parties through the use of appropriate security measures.

(c) Any information shared in accordance with this ISA must only be retained for as long as strictly necessary for the purposes of the sharing set out in the Information Sharing Annex in Part C. In accordance with their respective retention policies, each Party shall regularly review Shared Information held by it to ensure that retention of the Shared Information is still required for the Purpose; any information that no longer needs to be retained, if requested by the Party providing the information, shall be returned to that Party or, securely deleted, destroyed, or erased (including all copies whether paper or electronic).

(d) All electronic data must be destroyed in an appropriate manner which renders it irretrievable. This could be logically, physically, digitally, or magnetically destroyed.

(e) All paper documents should be immediately strip shredded or incinerated.

7.11 Where Parties rely on consent as the condition for processing personal data then withdrawal of consent means that the condition for processing will no longer apply. Withdrawal of consent shall be communicated to the other Parties and processing must cease as soon as possible.

7.12 This ISA does not give licence for unrestricted access to information another Party may hold. It sets out the parameters for the safe and secure sharing of information for a justifiable need to know purpose.

7.13 No Party shall process or otherwise transfer any of the Shared Information outside of the United Kingdom without the written approval of the original owner of the information (the original owner being the party who collected the information).

7.14 It is the responsibility of each Party to ensure that its staff with authorised access to any Personal Data covered by this ISA, are aware of their obligations under the Data Protection Legislation to safeguard that information. Staff must be aware that breach of the controls contained within this ISA could be a matter for internal disciplinary action. It may also provide grounds for a complaint under the Data Protection Legislation against them personally which may result in criminal or civil action.

7.15 Parties will not allow access to systems or information of another data controller in contravention of this ISA.

7.16 In the event of any information security breach in respect of Shared Information, the Party that is responsible for the security of that particular information will immediately take steps to contain the breach once it has been identified. If that Party decides that the Information Commissioner's Office should be notified of the breach under Article 33(1) UK GDPR, the Party will also notify the other Parties as part of that process. Each Party shall provide reasonable cooperation and assistance to the Party in respect of any information security breach.

7.17 Once the breach referred to in Clause 7.16 above has been contained, the relevant Party will launch an investigation to establish the reasons behind the breach and will share the outcome of the investigation with the other Parties it determined are relevant.

8 Review of this ISA

8.1 The Parties shall regularly review the ISA to ascertain whether it is still required. If the ISA is no longer required, the Parties may exercise their rights under Clause 9 to terminate the ISA.

8.2 If the information sharing is no longer required, any Party may exercise their rights under Clause 9 to withdraw from this ISA.

8.3 This ISA will be reviewed 12 months after the Commencement Date then yearly thereafter.

8.4 This review is the joint responsibility of the Parties and should be carried out by the SPoC for each Party.

9 Withdrawal or termination from ISA

9.1 If any Party wishes to withdraw from this ISA, it must give at least six (6) weeks' written notice to the other Parties.

9.2 The withdrawing Party shall ensure that all Shared Information held by it is reviewed and, where possible, securely deleted without delay. Where it is not possible to securely delete the Shared Information in this way, the withdrawing Party shall retain and securely delete the Shared Information in accordance with its own data retention policy.

9.3 The Parties may at any time mutually agree to terminate this ISA on a date to be agreed between the Parties. In such event, all Parties shall ensure that all Shared Information held by it is reviewed and, where possible, securely deleted without delay. Where it is not possible to securely delete the Shared Information on termination of this ISA, each Party shall retain and securely delete the Shared Information in accordance with its own data retention policy.

9.4 If a Party finds or reasonably suspects that any other Party may not be complying with this ISA it reserves the right to refuse to provide Shared Information to that other Party whilst resolving any dispute between the Parties in accordance with Clause 13.5 below.

9.5 Information quality needs to be of a standard fit for the purpose information is to be used for, be complete, accurate and as up to date as required for the purposes for which it is being shared. Parties must ensure that the Personal Data, Special Categories of Personal Data and Criminal Conviction Data that they hold are processed in accordance with DPA principles. This includes ensuring that the Data is accurate, complete, and up-to-date and is not kept any longer than is necessary.

9.6 Parties undertake that information meets a reasonable quality level for the proposed purposes for which it is being shared and are able to evidence this.

9.7 Parties' employees processing information shared under this ISA will be trained to a level that enables them to undertake their duties confidently, efficiently, and lawfully. This is an obligation on Parties and responsibility for it cannot be assigned to another organisation, although delivery of training can be with that third party's consent.

9.8 Parties may collaborate in the development and delivery of training.

9.9 Refresher training shall be undertaken annually, to include a DP update and any necessary system training updates.

10 Suspension

10.1 Any Party can suspend this ISA immediately by notice in writing for a period of up to 45 days if it reasonably believes that security has been seriously breached. A notice of suspension must be in writing to all the other Parties and state the reasons for believing there has been a serious breach of the ISA and the period of the suspension. During the period of suspension, a risk assessment will be undertaken and a resolution meeting convened, the panel of which will be made up of the signatories to this ISA or their nominated representative. This meeting will take place within 14 days of the suspension.

11 Contact details for key members of staff

11.1 Any notices, communications, or complaints in respect of this ISA must be in writing and shall be addressed to the relevant Party's Single Point of Contact.

12 Audit

12.1 Any Party has the power to audit any other Party to ensure compliance with the provisions of this ISA.

12.2 The Party conducting the audit shall:

- provide at least 5 Working Days' notice of its intention to conduct an audit, unless prevented from providing such notice by law;
- comply with security, sites and facilities operating procedures applicable to any sites or information being audited;
- use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the other Party; and
- bear its own respective costs and expenses incurred in respect of the audit

12.3 The Party who is the subject of the audit shall:

- grant to the Party conducting the audit and their respective authorised agents the right of reasonable access to relevant records, sites and materials and shall provide all reasonable co-operation and assistance; and
- shall bear their own respective costs and expenses incurred in respect of compliance with its obligations under this clause.

13 General

13.1 This ISA shall begin on the Commencement Date and shall continue until terminated in accordance with Clause 9.

13.2 No variation to the terms of this ISA shall be effective unless in writing and signed by an authorised signatory of each of the Parties.

13.3 Each Party shall take reasonable steps to ensure the reliability of their respective employees, agents or contractors who may have access to the Shared Information, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Shared Information, as strictly necessary for the Stated Purpose, and to comply with applicable laws in the context of that individual's duties to the relevant Party, ensuring that all such individuals are subject to confidentiality undertakings and a processing agreement where appropriate.

13.4 Nothing under this ISA shall create, or be deemed to create, a partnership or the relationship of employer and employee between the Parties.

13.5 In the event that any dispute arises between the Parties in connection with this ISA, the Parties shall, in the first instance, use their reasonable endeavours to resolve it amicably between them. If the dispute is not resolved between each Party's representatives within twenty eight (28) days of the Party raising the dispute gives written notification to the other Party or all the other Parties with whom the Party is in the dispute , the matter shall be referred to a meeting of each Party's relevant senior officers or chief executives for resolution.

13.6 Each Party shall remain liable for any losses or liabilities incurred due to their own or their employee's actions and neither Party intends that any other Party shall be liable for any losses or liabilities incurred as a result of the defaulting Party's breach of this ISA.

13.7 This ISA is not intended to be legally binding, and no legal obligations or legal rights shall arise between the Parties from this ISA. The Parties enter into the ISA intending to honour all their obligations.

13.8

Part C - Information Sharing Annex

FOR USE WHERE THE PARTIES ARE SHARING INFORMATION SUBJECT TO THE UK GDPR AND PARTS 1 & 2 OF THE DPA 2018

Title of initiative: NCSAB Safeguarding Adults Board and Sub-Groups

Particulars of the information sharing initiative

1. Why is the information being shared?
The Nottingham City Safeguarding Adults Board and its sub-groups share personal data for the purposes of commissioning, completing, and providing assurance for Safeguarding Adults Reviews (SARs).The Board has certain Core members; the City Council, the County Council, the Police and the CCG. Non-statutory partners such as Framework are also invited to attend. In particular, the Parties will share information in connection with SARs commissioned in cases of people who have been seriously harmed as a result of abuse or neglect, whether known or suspected, and there is concern that partner agencies could have worked more effectively to protect the adult. This also includes those adults who have died while sleeping rough or are vulnerably housed; in these cases there will often be a increased need for information to be shared between the Parties as there not be one single identifiable host local authority due to changes in address. There are a number of Sub-Groups sitting below the NCSAB which exist to support the main Board with carrying out its functions. which also share information for the same purposes as the main Board. These are as follows: • The SAR Sub-Group – processes referrals and provides confirmation that SAR criteria is met • The Quality Assurance Sub-Group – assuring Board of quality of SARs • The Training, Learning and Information Sub-Group – to implement learning from SARs

2. What information is being shared?		
Personal Data	**Special Category Data**	**Criminal conviction or allegations data ✓**

-Name and contact details of citizen who is subject of the SAR -Address and contact details -All circumstances of deaths or incidents of harm -Any social care information about the individual -Names and job details of all professionals involved -Details of associated persons such as family members	Racial or ethnic origin ✓ Political opinions Religious or philosophical beliefs ✓ Trade union membership genetic biometric health ✓ (including social care needs, mental health and substance abuse) Sex life or sexual orientation ✓	☐ If you tick this, also complete Part C3 below:

3. What is the legal basis for sharing the information (additional to Clause 5 of the ISA)? (Tick as appropriate)

The lawful basis for processing and sharing the information is set out in Clause 5, namely that

The lawful basis for processing **special category data** is: (Tick as appropriate)

Explicit consent	Not for profit body	Substantial public interest ✓
Employment social security, social protection ✓	Made public by the data subject	Medicine, Employee capacity, medical diagnosis, health or social care
Vital interests	Legal claims and judicial function	Archiving, research or statistical

If relying on 'Substantial Public Interest' for processing special category data, the condition(s) for doing this are: (Tick as appropriate)

Confirm Appropriate Policy Document in place for:	
Nottingham City Council	✓

Statutory and Government Purposes	✓
Administration of justice and parliamentary purposes	
Equality of opportunity or treatment	
Racial and ethnic diversity at senior levels of organisations	
Preventing or detecting unlawful acts	✓
Protecting the public against dishonesty	✓
Regulatory requirements relating to unlawful acts and dishonesty	
Journalism, academic purposes, artistic purposes and literary purposes in connection with unlawful acts and dishonesty	
Preventing fraud	
Suspicion of terrorist financing or money laundering	
Support for individuals with a particular disability or medical condition	
Counselling	
Safeguarding of children and individuals at risk	✓

Safeguarding of economic well-being of certain individuals	
Insurance	
Occupational pensions	
Political parties	
Elected representatives responding to requests	
Disclosure to elected representatives	
Informing elected representatives about prisoners	
Publication of legal judgments	
Anti-doping in sport	
Standards of behaviour in sport	

The lawful basis for processing **criminal conviction and allegation data** is:
S 10(4) and (5) provides all the conditions in Parts 1, 2 and 3 of Schedule 1; 33 conditions in all. Another 10 are provided by virtue of paragraph 36 which allows reliance on all the substantial public interest conditions in Part 2 without the substantial public interest. Another 2 are provided by paragraph 37.

4. Security Requirements

Information is mainly shared via email. Where possible and to the extent that it does not conflict with any of the other provisions set out in this ISA, each Party shall ensure that any Personal Data, Special Categories of Personal Data or Criminal Conviction Data contained within the Shared Information is anonymised or pseudonymised.

All information transmitted across public networks within the UK or across any networks overseas must sent by secure email which meets UK central government's connection standards or be encrypted using appropriate software (e.g. Microsoft 365, Egress Switch, Cryptshare, etc.).

Passwords must be sent separately to the information exchanged and must provide the correct level of security taking all factors into account, including the nature of the data being shared. Passwords must be changed regularly, and the Parties' respective password arrangements will include provisions to avoid the use of weak or predictable passwords.

5. Single Point of Contact (SPoC)

As specified in the details of Parties in the annex below.

6. Status of Parties (joint controllers, processors)

Each Party is a data controller. None of the Parties is a data processor acting on behalf of any other Party.

Additional information

None.