[PROJECT NAME/PURPOSE/SERVICES]

Information Sharing Agreement between

MANCHESTER CITY COUNCIL

and

[INSERT NAME(S) OF PARTY(IES)]

|  |
| --- |
| **GUIDANCE FOR COMPLETING THIS ISA**  This ISA is designed for use on simpler projects.  To ensure the Contents page numbers remain correct please ensure you update this Table of Contents post completion. To do this right click anywhere in the Table, then select “Update field”. In the window select “update entire table”. Once done please delete this highlighted text.  Where text requires amendment it will be highlighted in red and contained within [square brackets].  Once the document has been completed, please ensure that all guidance notes are deleted, [square brackets] are deleted, text is changed to Ariel Font size 12 (save for the front cover) and the Automatic colour is used. |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description of change** |
| 1.00 |  |  | Approved version |
| 1.01 | 23/03/2018 |  | GDPR update based upon Data Protection Bill |
| 2.00 | 11/06/2018 |  | Updated for DPA 2018 |

# 

**TABLE OF CONTENTS**

[FOREWORD 4](#_Toc509824810)

[1 PARTIES 4](#_Toc509824811)

[2 PURPOSE OF ISA 4](#_Toc509824812)

[3 PURPOSE AND LEGAL BASIS FOR DATA SHARING 5](#_Toc509824813)

[4 SPECIFIED PERSONAL DATA 8](#_Toc509824814)

[5 LAWFULLNESS, FAIRNESS, TRANSPARENCY 10](#_Toc509824815)

[6 TECHNICAL AND ORGANISATIONAL SECURITY MEASURES 11](#_Toc509824816)

[7 SECURE METHOD OF TRANSFER 12](#_Toc509824817)

[8 DATA QUALITY AND ACCURACY 12](#_Toc509824818)

[9 OTHER USES/DISCLOSURE 13](#_Toc509824819)

[10 RETENTION AND DISPOSAL 13](#_Toc509824820)

[11 SECURITY BREACH PROCEDURES AND NOTIFICATION 13](#_Toc509824821)

[12 SUBJECT ACCESS RIGHTS AND COMPLAINTS 13](#_Toc509824822)

[13 MAIN CONTACTS – RESPONSIBILITIES 14](#_Toc509824823)

[14 FREEDOM OF INFORMATION 14](#_Toc509824824)

[15 DEFINITIONS AND INTERPRETATION 14](#_Toc509824825)

[16 COMMENCEMENT AND TERMINATION 15](#_Toc509824826)

[17 REVIEW 15](#_Toc509824827)

[18 AUTHORISATION 15](#_Toc509824828)

[ANNEX 1 – GLOSSARY OF TERMS 16](#_Toc509824829)

[ANNEX 2 – DATA PROTECTION PRINCIPLES 20](#_Toc509824863)

[ANNEX 3 – DPA 2018 CONDITIONS OF PROCESSING 21](#_Toc509824864)

## FOREWORD

Each Party is legally responsible for ensuring that their use of personal data is lawful, properly controlled and upholds the rights of individuals. Evidencing these controls and safeguards (in the form of ‘who, what, where, when and how’) provides the Parties to this ISA and the citizens we serve with the confidence and assurance that data sharing is:

• consistent with all relevant legislation, professional and industry codes;

• in compliance with the principles relating to processing of personal data under Article 5 of the General Data Protection Regulation and documents the parties respective responsibilities for compliance under GDPR Article 26;

• governed by strict rules designed to protect the security and confidentiality of the personal data throughout the data sharing life cycle (privacy by default and design);

• overseen and monitored by accountable senior managers responsible for ensuring compliance and that staff are properly trained;

• respectful of individual privacy and the rights of individuals.

# 1 PARTIES

1.1 This Information Sharing Agreement (ISA) is between Manchester City Council and [inset name(s) of other party(ies)].

1.2 Each Party to this ISA is a separate Controller responsible in Law for determining the purposes for which and the manner in which any Personal Data are or are to be processed.

# 2 PURPOSE OF ISA

2.1 This ISA outlines the Parties’ intentions when sharing the Specified Personal Data for the [insert name of project/contract/services]. This includes:

* the purpose and legal gateway permitting the sharing;
* the Specified Personal Data to be shared;
* how the Specified Personal Data is to be shared.
* the legislative and information standards governing the sharing, security, use and retention of disclosed information, including governance controls, security and security breach notification requirements and the rights of Data Subjects

2.2 An ISA does not of itself make the sharing of Personal Data lawful. Nor does the existence of a legal gateway override the need to comply with the Common Law Duty of Confidence and other relevant Law.

2.3 This ISA therefore evidences how these legal requirements are to be addressed providing the Parties with assurance that agreed governance controls are in place to ensure that Personal Data sharing is managed appropriately and in conformance with the Law.

# 3 PURPOSE AND LEGAL BASIS FOR DATA SHARING

3.1 Specified Personal Data may be shared on a proportionate and necessary basis for each of the purposes under the corresponding legal authority set out below:

|  |  |
| --- | --- |
| **Purpose** | **Legal authority** |
|  | The general power of competence in Section 1 of the Localism Act 2011 |
| [add additional as relevant] | [add additional as relevant] |
|  |  |
|  |  |

3.2 Article 6 (1) of the GDPR says that Processing shall be lawful only if one of a number of conditions apply. For the purposes of this ISA the following condition[s] [apply/applies:] **Tick all that apply**

**Article 6 (Lawfulness of processing)**

Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes. ;**\*\*consent is unlikely to be an appropriate condition of processing as consent must be demonstrable, freely given and as easily withdrawn.\*\***
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. ;
3. processing is necessary for compliance with a legal obligation to which the controller is subject. ;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person. ;
5. 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. ;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. ;**\*\*This condition shall not apply to processing carried out by public authorities in the performance of their tasks \*\*.**

3.3Disclosures may be made by either Party to another local authority or other public body where on a case by case basis it is considered necessary to set aside an obligation of confidence in the interests of:

* + - Safeguarding vulnerable adults or children;
    - Reducing risk to individuals, service providers and the public as a whole;
    - The prevention and detection of crime.

3.4Article 9 GDPR prohibits the processing of special categories of personal data unless one of a number of conditions apply. For the purposes of this ISA the following condition[s] apply/applies:- **Tick all that apply**

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes. ;*\*\*consent is unlikely to be an appropriate condition of processing as consent must be demonstrable, freely given and as easily withdrawn.\*\**
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; ; This will apply if the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection. See Data Protection Act 2018 Schedule 1 Part 1 condition 1.
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

This will apply where the Council has an appropriate policy document and the processing is necessary for one of the following purposes:-

* The exercise of a function conferred on a person by an enactment or rule of law;
* The processing is of specified personal data (ethnic origin, religious or philosophical beliefs, data concerning health and/or an individual’s sexual orientation) for the monitoring equality of opportunity or treatment and does not involve measurers and decisions with respect to a particular individual;
* The processing is for the purposes of prevention or detection of an unlawful act and must be carried out without the consent of the data subject.
* The processing is for the purposes of protecting the public against dishonesty, improper conduct, unfitness or incompetence and must be carried out without the consent of the data subject
* The processing is to meet regulatory requirements relating to unlawful acts and dishonesty.
* The processing is for the prevention of fraud and involves disclosure to an anti-fraud organisation in accordance with its arrangements.
* The processing is for the purposes of protecting a child or person at risk from neglect or harm or protecting their physical, mental or emotional wellbeing where consent cannot be given in the circumstances, cannot be reasonably expected to be obtained or to obtain consent would be prejudicial to the purpose.
* The processing is of data concerning health and is for protecting the economic well-being of an individual over 18 from economic risk where consent cannot be given in the circumstances, cannot be reasonably expected to be obtained or to obtain consent would be prejudicial to the purpose.

1. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards;  This will apply if the processing is necessary for health or social care purposes. See Data Protection Act 2018 Schedule 1 Part 1 condition 2.
2. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;  This will apply if the processing is necessary for reasons of public interest in the area of public health, and is carried out by or under the responsibility of a health professional, or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law. See Data Protection Act 2018 Schedule 1 Part 1 condition 3.
3. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.  This will apply if the processing is necessary for archiving purposes, scientific or historical research purposes or statistical purposes, is carried out in accordance with Article 89(1) of the GDPR and is in the public interest. See Data Protection Act 2018 Schedule 1 Part 1 condition 4.

or

1. This ISA does not involve any Special Categories of Personal Data. A condition of processing under Article 9 is not required.

3.5 Article 10 of GDPR states that processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. For the purposes of this ISA the following condition[s] apply/applies:-

Under Section 10(5) of the DPA 2018 personal data relating to criminal convictions and offences must meet a condition in Part 1, 2 or 3 of Schedule 1 of the DPA 2018

**Schedule 1 Part 1**

1. Employment, social security and social protection ;
2. Health and social care ;
3. Public health ;
4. Research etc. ;

**Schedule 1 Part 2**

1. Statutory etc. and government purposes. ;
2. Administration of justice and parliamentary purposes. ;
3. Equality of opportunity or treatment. ;
4. Preventing or detecting unlawful acts. ;
5. Protecting the public against dishonesty. ;
6. Regulatory requirements relating to unlawful acts and dishonesty etc. ;
7. Preventing fraud. ;
8. Safeguarding of children and of individuals at risk. ;
9. Safeguarding of economic well-being of certain individuals. ;

**Schedule 1 Part 3**

1. Consent. ;
2. Protecting individual’s vital interests. ;
3. Processing by not-for-profit bodies. ;
4. Personal data in the public domain. ;
5. Legal claims. ;

or

This ISA does not involve data involving criminal convictions etc., a condition of processing under Article 10 is not required. .

4 SPECIFIED PERSONAL DATA

4.1 For the purpose of this ISA, the Specified Personal Data referred to in Section 3 above are:

|  |  |
| --- | --- |
| Type of Personal Data | [Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.] |
| Type of Special Categories of Personal Data |  |
| Type of Personal Data relating to criminal convictions and offences or related security measures |  |
| Categories of Data Subject | [Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.] |

4.2 No more than the absolute minimum necessary Specified Personal Data will be shared observing the “need to know” principle taking account of the nature and circumstances in which the Personal Data were obtained.

# 5 LAWFULLNESS, FAIRNESS, TRANSPARENCY

5.1 In line with the legal obligation under the Data Protection Legislation at the earliest point of contact the Data Subject will receive a Privacy Notice from [insert name of other party] ensuring that they are informed about the information collected and recorded about them, the persons or organisations with whom it may be shared, and the purposes of the sharing.

|  |
| --- |
| \*\*Under A13 a privacy notice is required when collecting personal data from the Data Subject. Where the sharing is in accordance and consistent with that notice the Council will not be required to send a further notice. Where the sharing is for a purpose other than that for which it was collected then an additional notice will be required\*\* |

# 6 TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

6.1 The Parties shall ensure that irrespective of whether Specified Personal Data is in transit or at rest, it is handled in compliance with all relevant legislation and recognised industry information security standards.

6.2 Appropriate technical, security and organisational measures shall be taken to safeguard against unauthorised or unlawful Processing of the Specified Personal Data and against accidental loss or destruction of, or damage to, the Specified Personal Data.

6.3 These measures shall cover all aspects of information governance, data handling and information security addressing organisational and technical controls such as physical security, system specific security, access privileges, staff reliability and training, including but not limited to ensuring:

* the controls deployed (including the method to be agreed for securely exchanging the Specified Personal Data) are appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Specified Personal Data based on the nature and sensitivity of the Specified Personal Data;
* access to Specified Personal Data complies with the “need to know” principle;
* where the Specified Personal Data is held on portable devices, appropriate encryption is deployed;
* where Specified Personal Data is stored or transported in paper form physical security safeguards are in place;
* all reasonable steps are taken to establish the reliability of employees (including permanent, temporary, placements, agency staff, consultants or volunteers) authorised to access the Specified Personal Data (including appropriate vetting of prospective employees, in accordance with recognised industry practice);
* employees authorised to access Specified Personal Data have received appropriate training in the Law of data protection and information security;
* contracts and/or organisational policies and codes ensure employees understand their duty of care and confidentiality obligations, including the circumstances in which unauthorised access or inappropriate disclosure of Personal Data may give rise to:
  + - * disciplinary measures if confidentiality is breached or Specified Personal Data information is knowingly or recklessly processed in a manner in contravention of the Law
      * the commission of a criminal offence under s.170 or s171 of the DPA 2018 if accessing or obtaining Personal Data without authorisation;
        + reasonable steps are taken to maintain and audit compliance with above measures.

6.4 Where a Party engages a Processor to process the Specified Personal Data it will ensure that the Processor provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the Data Protection Legislation and ensure the protection of the rights of the Data Subject.

# 7 SECURE METHOD OF TRANSFER

7.1 Specified Personal Data shall be transferred by a secure method to be agreed between the Parties. This agreed secure method will be documented.

7.2 The Specified Personal Data shall be transferred at the following times and frequencies:

[insert as applicable]

# 8 DATA QUALITY AND ACCURACY

8.1 Each Party is responsible for the quality and accuracy of the Specified Personal Data it obtains, uses and discloses.

8.2 [Before exchanging Specified Personal Data, common identifiers (excluding National Insurance Numbers) will be agreed to limit the potential for avoidable mismatches.]

8.3 If a Party later discovers information is inaccurate, it will take reasonable steps to inform other recipients to enable the correction or updating of their records/case management systems.

# 9 OTHER USES/DISCLOSURE

9.1 No Specified Personal Data will be used for purposes other than those outlined in Section 3 of this ISA or disclosed to a third party unless permitted or required by Law.

9.2 In no circumstances will Specified Personal Data be used/disclosed for the purpose of marketing unsolicited products and/or services.

# 10 RETENTION AND DISPOSAL

10.1 The Specified Personal Data shall not be retained longer than is necessary.

10.2 Once no longer required for the purpose, the Specified Personal Data shall be securely disposed of in accordance with each Party’s documented retention and disposal policies.

# 11 SECURITY BREACH PROCEDURES AND NOTIFICATION

11.1 Each Party confirms it has established Incident Reporting and Management procedures consistent with the Data Protection Legislation and the Information Commissioner’s guidance for investigating and handling security breaches.

11.2 In the event of a breach of security or confidentiality resulting in the compromise of any Specified Personal Data, urgent remedial measures will be implemented, including notifying the Party from whom the Specified Personal Data has been obtained.

11.3 Where required by Data Protection Legislation, the Parties acknowledge that it may be necessary to notify Data Subjects and/or relevant regulatory bodies of the breach.

# 12 SUBJECT ACCESS RIGHTS AND COMPLAINTS

12.1 Under Data Protection Legislation, Data Subjects are entitled to know what information is held about them, by whom and for what purpose and, if it is not accurate to ask for it to be corrected. They can also ask for Processing to be restricted where they believe the information is inaccurate or being inappropriately processed and for automated decisions to be reviewed.

12.2 In the event of a request concerning any Data Subject right under Data Protection Legislation or a complaint relating to the Processing of Specified Personal Data, the receiving Party will in accordance with the Data Protection Legislation take steps to notify and consult with the Party from whom the Specified Personal Data was obtained. The Parties acknowledge that a Data Subject may exercise his or her rights under the Data Protection Legislation against either Party.

12.4 Each Party acknowledges their responsibility to ensure adequate resources are committed to handling data protection related requests and that these are processed within statutory time limits and/or in line with local customer services and complaint policies.

# 13 MAIN CONTACTS – RESPONSIBILITIES

13.1 Each Party shall ensure it has a Lead Officer who is the main point of contact for the other Party.

13.2 The Lead Officers will liaise on operational arrangements and in line with Section 7.1 will establish the method for securely exchanging Specified Personal Data after first taking advice from their own IT Security and Information Governance leads.

# 14 FREEDOM OF INFORMATION

14.1 [As public authorities for the purposes of the FoIA, the Parties to this ISA acknowledge their responsibilities in relation to handling requests for information.]

|  |
| --- |
| \*\*If both parties public authorities\*\* |

14.2 In line with the Section 45 FoIA Code, the Parties shall cooperate with each other in the event of receiving requests for information about or shared under this ISA.

# 15 DEFINITIONS AND INTERPRETATION

15.1 Annex 1 outlines the relevant definitions applicable to this ISA.

15.2 All data protection terms shall be interpreted in accordance with the meaning ascribed to them in the Data Protection Legislation.

15.3 This ISA is not intended to be legally binding and no legal rights shall arise between the Parties from these provisions save that it is acknowledged that once Specified Personal Data is lawfully and securely transferred, the recipient assumes the responsibilities as Controller for ensuring that Specified Personal Data is processed in accordance with the data protection principles in the Data Protection Legislation identified in Annex 2.

# 16 COMMENCEMENT AND TERMINATION

16.1 This ISA shall take effect from the date the Parties fix their signatures below and shall continue in force until [date] [such time as [insert circumstance]] or this ISA is terminated by either Party.

# 17 REVIEW

17.1 This ISA will be reviewed every [x years].

# 18 AUTHORISATION

Signed for and on behalf of Manchester City Council

|  |  |
| --- | --- |
|  |  |
|  | (Signature) |
| Name: | [INSERT NAME OF SIGNATORY] |
| Position | [INSERT POSITION OF SIGNATORY] |

Signed for and on behalf of [insert party]

|  |  |
| --- | --- |
|  |  |
|  | (Signature) |
| Name: | [INSERT NAME OF SIGNATORY] |
| Position | [INSERT POSITION OF SIGNATORY] |

# ANNEX 1 – GLOSSARY OF TERMS

|  |  |
| --- | --- |
| Term | Definition |
| Common Law Duty of Confidence | An obligation or expectation of confidence is not absolute and information may be lawfully disclosed:• if the person owed the duty, gives consent;• in compliance with a court order or legal obligation;• where the public interest in disclosure overrides the public interest in the protection of the confidence. |
| Controller | means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of personal data |
| Data Protection Legislation | (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 subject to Royal Assent to the extent that it relates to Processing of personal data and privacy; (iiii) all applicable Law about the Processing of personal data and privacy |
| Data Subject | an identified or identifiable natural person who can be identified, directly or indirectly from the personal data. |
| DPA 2018 | Data Protection Act 2018. |
| FoIA | Freedom of Information Act 2000. |
| GDPR | General Data Protection Regulation *(Regulation (EU) 2016/679)* |
| Law | Law : means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which either Party is bound to comply |
| LED | Law Enforcement Directive (Directive (EU) 2016/680) |
| Party or Parties | means a party to this ISA. |
| Personal Data | means personal data within the meaning of the Data Protection Legislation which relates to a Data Subject in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| Privacy Notice | notices which are used to inform Data Subjects how their Personal Data is to be used and with whom it will be shared and why. This ensures that the Processing is undertaken lawfully, fairly and in a transparent manner. |
| Processing | means any operation or set of operations which is performed on Personal Data, by computer or any other means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction |
| Section 45 FoIA Code | means the Code of Practice on the discharge of public authorities' functions under Part I of the Freedom of Information Act 2000 |
| Special Categories of Personal Data | means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. |
| Specified Personal Data | means the Personal Data and Special Categories of Personal Data identified in section 4 |

**E+W+S+N.I.**

# ANNEX 2 – DATA PROTECTION PRINCIPLES

Article 5

Principles relating to Processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the Data Subject (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

# ANNEX 3 – DPA 2018 CONDITIONS OF PROCESSING

[Data Protection Act 2018 - Schedule 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted)