Data Protection policy
CG14

Beware when using a printed version of this document. It may have been subsequently amended. Please check online for the latest version.

Applies to:	All NHS Resolution employees, Non-Executive Directors, secondees and consultants, and/or any other parties who will carry out duties on behalf of NHS Resolution. Contractors and panel firms are required to adhere to the terms of their contractual agreements.
Version:	4
IG Group review:	13th December 2023
SMT review:	3rd January 2024
Board approval:	24th January 2024 (approved offline on 16th February 2024, formally ratified at the 20th March 2024 Board meeting)
Next review date:	January 2027
Author:	Tinku Mitra, Deputy Director of Corporate and Information Governance
Owner:	Joanne Evans, Director of Finance and Corporate Planning

Contents

1. Introduction

The business of NHS Resolution involves the processing of information about individuals ("**personal data**"). Often, due to the nature of the work of the organisation, this information will include details many people would consider to be sensitive and/or private (for example, details about physical or mental health, performance at work, and financial affairs). In order to protect the rights and freedoms of individuals, to retain the trust of those with whom we are dealing and that of the wider public, and to minimise the risk of there being a successful legal challenge or regulatory action in relation to the way(s) in which the organisation processes personal data it is essential we act in accordance with the law in this area. We also aim to follow 'best practice' recommendations where this is feasible.

2. Purpose

The purpose of this policy is to set out, in broad terms, the requirements with which we need to comply in processing personal data, and how we go about complying with them. This policy (together with our other data protection policies, referenced in this document) forms our 'appropriate policy document' for the purposes of complying with requirements under the Data Protection Act 2018.Further information about how we implement this policy is within our guidance and other policies listed at the end of this policy.

3. Equality impact assessment

NHS Resolution aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It is a requirement that we conduct equality impact assessments on all policies and services within the organisation.

The purpose of the assessment is to minimise and, if possible, remove any disproportionate impact on employees on the grounds of race, sex, disability, age, pregnancy and maternity, marriage and civil partnership, gender reassignment, sexual orientation, religious or other belief. As part of its development, this Policy and its impact on equality have been reviewed in consultation with trade union and other employee representatives in line with NHS Resolution's equality impact assessment tool (Appendix 1).

4. The UK data protection legislation

The two key pieces of legislation, which govern data protection in the UK (the data protection legislation), are:

(i) The UK General Data Protection Regulation (UK GDPR); and

(ii) The Data Protection Act 2018 (DPA 2018).

Definitions – for the purposes of the data protection legislation:

- **Personal data:** Data relating to a living individual who can be identified from the data, directly or indirectly.

  The data may 'relate to' the identifiable living individual, whether in personal or family life, business or profession.**Special categories of personal data:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, and genetic data, biometric data when used to identify a person, data concerning health or a data subject's sex life or sexual orientation.

- **Processing:** Processing, in relation to information or data, means operations 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.

- **Data subject:** Data subject means "an individual who is the subject of personal data". A data subject must be a living individual. A data subject need not be a United Kingdom national or resident. Generally, in the exercise of its functions, individuals we interact with (for instance, our employees, clinicians working with the Practitioner Performance Advice service, or those bringing claims against the NHS) are 'data subjects'.

  Please note that whilst the data protection legislation does not apply to information relating to the deceased, confidentiality obligations continue to apply to such data. This is supported within the DHSC Confidentiality Code of Practice and should be followed by all NHS Resolution staff.

- **Data controller:** Data controller means a person or organisation (including a public authority) "which, alone or jointly with others, determines the purposes and means of the processing of personal data".

  A data controller decides how and for what purpose personal data is to be used. Generally, in the exercise of its functions, NHS Resolution acts as a 'data controller'.

- **Data processor:** Data processor, in relation to personal data, means any person or organisation which processes the data on behalf of the data controller.

  A data processor will undertake tasks in accordance with a data controller's instructions. They must not use the data for any other purpose.

5. Roles and responsibilities

- **Chief Executive and Accounting Officer:** Accountable for all information governance matters including compliance with the requirements of the data protection legislation.

- **Audit and Risk Committee:** Has responsibility for assurance on the strategic processes for risk identification, control and governance.

- **Information Governance Group:** Led by the SIRO to discuss and make key decisions regarding information governance and security matters for the organisation. A summary of duties include:
    - To act as a focus for information governance within NHS Resolution including lessons learnt, good practice and IG communications;
    - To consider data sharing requests (internal and external) from across the functions of NHS Resolution which raise issues around data protection and/or information governance.

- **Senior Information Risk Owner (SIRO):** The SIRO takes ownership of the organisation's information risk and acts as an advocate for information risk on the NHS Resolution Board and Senior Management Team, providing advice where necessary. Further responsibilities include, but are not limited to:

    - Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its clients and stakeholders;
    - Owning the organisation's overall information risk policy and risk assessment processes, information incident management framework, and ensuring they are implemented consistently by the Information Asset Owner (IAO);
    - Advising the Chief Executive and Accounting Officer on the information risk aspects of internal controls.

- **Caldicott Guardian:** Caldicott Guardians help their organisations to ensure that confidential information about health is used ethically, legally, and appropriately. They help to protect each patient and service user's right to confidentiality. The Director of Safety and Learning fulfills this role for NHS Resolution.

- **Data Protection Officer (DPO):** The DPO has specific statutory responsibilities (as set out in Article 39 of the UK GDPR) as well as responsibilities defined by the organisation. These responsibilities include, but are not limited to, the following:

    - Educating the organisation on important compliance matters;
    - Training staff involved in data processing;
    - Conducting audits to ensure compliance and address potential issues in a proactive manner;
    - Acting as the point of contact between NHS Resolution and the Information Commissioner's Office (ICO);
    - Maintaining records of all data processing activities conducted by NHS Resolution;
    - Providing advice on Data Protection Impact Assessments (DPIAs).

- **Head of Technology and Operations & Information Security Officer (ISO):** The ISO is a security leadership role with a core responsibility to drive and deliver NHS Resolution's security strategy and implement the Information Security Management System (ISMS). Reporting to the Chief Information Officer (CIO) the ISO has the following responsibilities:
    - Developing and implementing an organisational-wide cyber and information security strategy;
    - Documenting and disseminating information security policies, processes and procedures;
    - Managing responses to information security incidents and breaches;
    - Supporting Information Asset Owners on security matters and information security risk.

- **Information Access Manager and Information Access Officer:** Has responsibility for dealing with Subject Access Requests (SARs), and other information rights requests from data subjects, under the data protection legislation and for ensuring sufficient fair processing information (such as in the form of a privacy notice) is available to users of NHS Resolution services.

- **Line managers:** All line managers are responsible for the promotion of the principles of the data protection legislation outlined within this policy and associated policies, within their teams.

- **Employees:** All employees and secondees who are carrying out duties on behalf of NHS Resolution are responsible for adherence to the principles of the data protection legislation outlined within this policy and implemented in associated guidance and for reporting any related adverse incidents in line with CG11 – Incident Reporting Policy and Procedure.

6. Principles relating to the processing of personal data

The UK GDPR sets out seven key principles that NHS Resolution must comply with when processing personal data. We must:

A. Process personal data lawfully, fairly and in a transparent manner:

The UK GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing but rather to ensure that we process personal data fairly and without adversely affecting the data subject. For most of the processing we carry out regarding our services and functions, we are relying on our public functions and powers as our lawful purpose. Where the processing relates to our employees, we are relying on our contractual arrangements with employees, and our employment law obligations. Further information about our lawful purposes is set out in section 8 below.

NHS Resolution has set out why we process personal data relating to claims in our Privacy Notice which is on NHS Resolution's website at https://resolution.nhs.uk/how-we-use-your-data/ . In terms of employees, our privacy notice can be found https://resolution.nhs.uk/privacy-cookies/.

Our privacy notices help us to satisfy our transparency requirements, whereby we are required to provide detailed, specific information to data subjects when we collect their personal data. Many of our standard forms and documents will provide a link to the relevant privacy notice.

For the purposes of notification to the Information Commissioner, the Data Controller remains NHS Litigation Authority as the legal entity.

B. Collect personal data for specified, explicit and legitimate purposes and not further process it in any manner incompatible with those purposes (purpose limitation):

To comply with this principle, NHS Resolution must maintain a record of how it uses personal data and ensure this is reflected in its Privacy Notices. We cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purposes in advance. If a new use of personal data is proposed that is not already covered by our privacy information, steps must be taken to ensure appropriate notice is given to data subjects before any new processing takes place.

We also record processing activity in a register of data processing activity (ROPA), which is maintained by our DPO. If you want to use personal data for a new or different purpose from that for which it was obtained, you must first contact the DPO for advice on how to do this in compliance with both the law and this policy.

C. Ensure personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation):

We put in place a number of measures to achieve this, including:

1) We limit access within our systems to stop data being used for irrelevant purposes;

2) We have data retention policies which help us to ensure that unnecessary data is not kept;

3) We design our processes, forms, and systems so as not to capture data which is not necessary to our statutory functions;

4) We are subject to Court rules and other legal requirements that help to ensure that our data is adequate for our tasks.

It is the responsibility of all NHS Resolution employees to ensure that personal data processing is adequate and limited to what is proportionate to achieve NHS Resolution's public task. You may only process personal data when performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties.

D. Ensure personal data is accurate and, where necessary, up to date; and inaccurate personal data are erased or rectified without delay:

Where NHS Resolution obtain information either directly from the data subject or via a third party, they must ensure where it is possible to do so of the accuracy of that data. If the data subject informs NHS Resolution of a (factual) inaccuracy, consideration should be given to how the data may be amended to reflect this. If, as will often be the case, the data subject requests the 'correction' of data which is in dispute, such as differing accounts or versions of events, the original data should not be amended. The data is not considered 'inaccurate' and therefore does not need correcting. Instead, we should ensure that competing versions are recorded accurately.

E. Ensure personal data is not kept for longer than is necessary for the purposes for which the personal data are processed (storage limitation):

NHS Resolution should not retain identifiable information for longer than is required to fulfil the purposes for which it is collected, as per **CG16 - Records Management Policy.**

F. Keep personal data secure and protect it against unauthorised or unlawful processing:

NHS Resolution will maintain technical and organisational measures to prevent or manage foreseeable incidents and identified risks which may affect the secure processing of personal data, as set out in **ITFA05 Information Security Policy**. All employees will be kept aware of security issues associated with the processing of data, through training and other measures.

You must take steps to maintain the security of any personal data you are processing, and extra care must be taken when processing special category personal data. Data protection and confidentiality clauses must be formally defined and included within third party contracts, and appropriate due diligence as to their security arrangements must be performed.

You must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality: only people who have a need to know and are authorised to use the personal data can access it;

(b) Integrity: personal data is accurate and suitable for the purpose for which it is processed; and

(c) Availability: authorised users are able to access the personal data when they need it for authorised purposes.

We have measures in place which allow us to restore access to personal data in the event of any incidents, including through backup processes. We also regularly test and evaluate the effectiveness of the security measures we have in place.

When considering appropriate security of personal data, you must consider whether the following steps are appropriate:

- Anonymisation;
- Pseudonymisation - a technique that replaces or removes identifiable information in a data set, and keeps that information separate (note that the data is not anonymised and still constitutes 'personal data' for the purposes of the data protection legislation);
- Encryption;
- Password protection;
- Restricting access to only designated individuals;
- Regular monitoring of access.

G. Demonstrate our compliance with the above principles (accountability):

As well as complying with the above principles, NHS Resolution must be able to document that compliance. This includes appointing a suitable qualified DPO, conducting DPIAs, regularly training staff, having in place appropriate policies and privacy notices and implementing privacy into our everyday systems.

7. Personal data breaches

If there is a data security breach, we are required to report the breach to the ICO within 72 hours, unless the breach is unlikely to result in risk to the rights and freedoms of the data subject. Given the tight timeframe we have for making a report to the ICO, all data security incidents, or suspected data security incidents, whether they meet the threshold for reporting or not, must be reported through the incident reporting form.

NHS Resolution will then assess whether the breach is reportable under the NHS Digital Guide to the Notification of Data Security and Protection Incidents utilising the NHS Data Security and Protection Toolkit.

If a data breach is likely to create a high risk to the rights and freedoms of the data subject there is an obligation on us to notify the affected data subjects directly. Again, the assessment of whether this is required will be undertaken by the DPO.

If you know or suspect that a personal data breach has occurred, you should report the incident immediately and if appropriate a lead investigator will be appointed to investigate the matter. You should preserve all evidence relating to the potential breach.

8. Conditions for processing personal data

When NHS Resolution is processing personal data, it is obliged to ensure that the processing meets at least one of the permitted conditions under Article 6 of the UK GDPR. The precise condition to be met will depend upon the particular activity being undertaken by NHS Resolution. The Article 6 conditions are:

a. The data subject has given their consent to the processing for one or more specific purposes.

b. The processing is necessary for the performance of a contract to which the data subject is party, or for the taking of steps at the request of the data subject with a view to entering a contract (this includes employment contracts).

c. The processing is necessary to comply with a legal obligation.

d. The processing is necessary to protect the vital interests of the data subject or another.

e. The processing is necessary for the performance of a public task or in the exercise of official authority.

f. The processing is necessary for the legitimate interests of the data controller (except where unwarranted because of prejudice or legitimate interests of the data subject). (As a public authority, NHS Resolution cannot rely on this condition for processing in connection with its public functions.)

In most circumstances, NHS Resolution's processing of personal data will be in reliance on conditions (c) and (e) in relation to our functions.

When NHS Resolution is processing special category personal data, it must also ensure that one of the conditions in Article 9 of the UK GDPR are met. Those most relevant to NHS Resolution's activities are:

- The data subject has provided explicit consent
- Processing is necessary for legal obligations in relation to employment of social security law
- Processing is necessary for the establishment, exercise or defence of legal claims or wherever courts are acting in their judicial capacity
- Processing is necessary for one of the substantial public interest conditions set out in Schedule 1 to the DPA 2018, which includes statutory functions
- Processing is necessary for the provision of health or social care or treatment or the management of health or social care systems, and the information is subject to a binding obligation of confidentiality
- Processing is necessary for public health, such as ensuring high standards of quality and safety of health care.

Where personal data relates to alleged or actual criminal activity on the part of the data subject, it is necessary to meet the requirements of Article 10 of the UK GDPR and one of the conditions in Schedule 1 to the DPA 2018, such as where

processing is necessary for the prevention or detection of crime and must take place without the consent of the data subject.

9. Data Protection Impact Assessments

Where NHS Resolution is considering a new project or service change initiative, which will include the processing of personal data, consideration must be given by the project leadership team throughout the project development process to whether a Data Protection Impact Assessment (DPIA) needs to be completed.

DPIAs are a legal requirement for processing that is likely to be high risk and we will conduct screening exercises for projects to establish the degree of likely risk associated with the project. A DPIA is a systematic process which will help identify and minimise data protection risks. Our DPIAs will take account of compliance risks, and also broader risks to individuals' rights and freedoms, including the potential for any significant social or economic disadvantage and the prospects of physical, material or non-material harms.

Advice on DPIAs may be obtained from the DPO but it is the responsibility of the project team to complete the DPIA. Records of DPIAs shall be kept by the Information and Security Governance Manager and must be periodically updated for the life of a service/project.

DPIAs must be completed before projects go live and sign off is to be sought from the DPO, SIRO and Chief Information Officer (CIO). Approval must also be given by the Information Asset Owner to confirm that the department has accepted any residual risks to data, that may arise in the project. Ownership of the DPIA should sit with the IAO.

10. Individuals' rights

Data subjects have rights in relation to their personal data and NHS Resolution must ensure it has processes in place to allow data subjects to exercise these rights. Data subjects may make requests in writing or verbally. As well as the entitlement to be informed about NHS Resolution's use of personal data via its Privacy Notices, individual data subjects have the right to:

- request access to their own personal data (subject access request (SAR)) – see further below in section 11;
- ask us to rectify or complete any inaccurate or incomplete personal data;
- ask us to erase their personal data in certain circumstances (the right to be forgotten);
- ask us to restrict processing of their personal data in certain circumstances;
- ask us to transfer their personal data to another data controller in limited circumstances (data portability);
- object to our processing of their personal data where we are processing it for our public tasks or for legitimate interests;

- object to our processing of their personal data for the purposes of direct marketing;
- object to any decisions we have made about them which were made solely by automated means;
- withdraw consent to any processing of their personal data, where we were relying on their consent for such processing;
- complain to the ICO; and
- take legal action for compensation if they suffer any material or non-material damage (including distress) because of our alleged contravention of the data protection legislation.

11. Subject access requests

Individuals have the right under the data protection legislation to make a request in writing for a copy of the information we hold about them. This is called a subject access request (SAR). As well as access to their personal data, when they make a SAR, data subjects are also entitled to be given a description of the information we process about them, what it is used for, who it might be passed on to, and how long we retain it.

Any such request for information should be construed a subject access request, unless it can be handled in the normal course of business (e.g .a request for a duplicate copy of a letter or other correspondence previously issued to the data subject If you receive a SAR request, you must pass it to the Information Access Manager as soon as possible. Requests should ordinarily be dealt with within the statutory timescale of one calendar month, but we do have the ability to extent this timeframe by a further two months where appropriate.

We will take reasonable care to ensure information can be requested or is made available in an appropriate format for individuals with disabilities.

There are exemptions we can apply to personal data so that it can be withheld following a SAR, including where the information is legally privileged or where its disclosure would breach our data protection obligations to others.

For further detail please see **Guidance Note on handling Subject Access Requests** or contact the Information Access Manager.

12. Data sharing

Generally, NHS Resolution are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

We can only share personal data with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;

(d) the transfer complies with any applicable international data transfer restrictions (see below in section 13); and

(e) we have put in place a fully executed written contract which contains appropriate data sharing or processing provisions.

13. International data transfers

Data transfers outside the UK are restricted by the UK GDPR, to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

NHS Resolution may only transfer personal data outside the UK if one of the following conditions applies:

(f) the UK has issued regulations confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subject's rights and freedoms (this includes all countries in the European Economic Area – an up-to-date list can be found here: International data transfers | ICO);

(g) appropriate safeguards are in place such as standard contractual clauses approved for use in the UK;

(h) the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

(i) the transfer is necessary for one of the other reasons set out in the UK GDPR including:

  (i) the performance of a contract between us and the data subject;

  (ii) reasons of public interest;

  (iii) to establish, exercise or defend legal claims;

  (iv) to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; and

  (v) in some limited cases, for our legitimate interest.

Any request for data to be transferred internationally, or any situation where such a transfer may occur, should be referred to the DPO for advice before any data is sent.

The ICO guidance for international transfers is set out below:

A guide to international transfers | ICO

14. The Duty of Confidentiality

NHS Resolution will receive a significant amount of highly sensitive and confidential information as part of its public functions. This information given to NHS Resolution in confidence must not be disclosed without consent, unless there is a lawful basis for doing so, e.g. disclosure to a legal advisor or in connection with litigation, a requirement of law or there is an overriding public interest to do so.

Such confidential information is subject to a duty of confidence and, if it is disclosed unlawfully, legal action can be taken against NHS Resolution for breach of confidence. Confidential information will include, but is not limited to, medical information, personnel information, and commercially sensitive information relating to the business of the organisation.

NHS Resolution has a duty both under the common law and under the Human Rights Act 1998 to ensure that the confidential information it holds is not inappropriately disclosed.

See Confidentiality: NHS Code of Practice for further information.

15. The Regulatory Environment

The Information Commissioner's Office (ICO) is the UK's independent public authority set up to uphold information rights. They do this by promoting good practice, ruling on complaints, providing information to individuals and organisations and taking appropriate action when the law is broken.

The ICO enforces and oversees the following legislation:

- UK GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Environmental Information Regulations 2004

The ICO has extensive statutory powers to investigate an organisation's compliance with the data protection legislation, including compulsory audit powers, and also issues extensive guidance and codes of practice on how the obligations under the data protection legislation should be met.

Should an individual feel their rights under the data protection legislation have been infringed, they can complain to the ICO, who will investigate and determine whether there has been a breach of the data subject's rights. If there has, the ICO may require further action.

The ICO can also issue monetary penalties in the event of a serious breach of the data protection legislation - with the upper level of monetary penalty being £17,000,000 or 4% of global annual turnover, whichever is the higher.

The ICO also prosecutes data protection offences, such as the unlawful obtaining or disclosing of personal data, or the unlawful re-identification of de-identified data.

There are a number of tools available to the ICO for taking action to change the behaviour of organisations and individuals that collect, use and keep personal data. They include criminal prosecution, non-criminal enforcement and audit.

16. Training and support

NHS Resolution will provide appropriate training to all staff on information governance, including data protection through the Data Security Awareness - elearning for healthcare (e-lfh.org.uk).

Managers and other staff may request advice from the Corporate Governance Team should they require support with the implementation of this policy.

This policy should also be read in conjunction with the other policies set out in section 18.

17. Implementation and monitoring

This Policy will be reviewed every three years. There may also be a need to review the Policy in advance of the planned review date where there is a reason to do so such as a change in legislation or regulation, accepted audit recommendations, or outcome of learning from incidents.

The Policy and any subsequent updates will be implemented across the organisation including publication to the intranet (Connect) and external website (where required), informing staff of the new/updated document through communication channels such as weekly staff bulletin (This Week), providing support through training (if necessary).

The effective implementation of this policy will be monitored by NHS Resolution's Information Governance Group including review of related incidents reported and associated actions taken and risks arising.

18. Links to related documents

This policy should also be read in conjunction with the following policies

CG02	Information Governance Strategy
CG12	Complaints Policy and Procedure
CG11	Incident Reporting Policy and Procedure
CG15	Freedom of Information Policy and guidance document
CG16	Records Management Policy
ITFA02	Guidance for Working with Confidential or Sensitive Information
ITFA05	Information Security Policy
ITFA2	Guidance for using Encrypted USB devices and Email Attachments

19. Document control

Date	Author	Version	Reason for change
2020			
13/08/20	Tinku Mitra	V1.0	2020 Review
20/08/20	Tinku Mitra	V2.0	ORG review
26/08/20	Tinku Mitra	V3.0	IG group review
02/09/20	SMT	V3.0	SMT review
2023			
07/12/23	Capsticks review	V4.0	2023 review
13/12/23	IG Group	V4.1	2023 review
03/01/24	SMT	V4.2	2024 final version
24/01/24	Board	V4 Final	Approved offline on 16th February 2024 following 24th January Board meeting. Formally ratified at the 20th March 2024 Board meeting.

Appendix 1 - Equality impact assessment tool

No.	Does the document/guidance affect one group less or more favourably than another on the basis of:	Yes/No	Comments
1.	Race	No	
2.	Ethnic origins (including gypsies and travellers)	No	
3.	Culture	No	
4.	Nationality	No	
5.	Age	No	
6.	Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
7.	Gender	No	
8.	Gender reassignment	No	
9.	Marriage and civil partnership	No	
10.	Pregnancy and maternity	No	
11.	Religion and belief	No	
12.	Sex	No	
13.	Sexual orientation including lesbian, gay and bisexual people	No	
14.	Is there any evidence that some groups are affected differently?	No	
15.	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	N/A	
16.	Is the impact of the document/guidance likely to be negative?	No	
17.	If so, can the impact be avoided?	N/A	
18.	What alternative is there to achieving the document/guidance without the impact?	N/A	
19.	Can we reduce the impact by taking different action?	N/A	

Name/s and job title/s of individual/s who carried out the Assessment:	Date of the Assessment
Tinku Mitra, Deputy Director of Corporate and Information Governance	14th December 2023