Healthwatch Richmond

Information Security & Governance Policy

Version: 1.1

Mike Derry April 2024

# Introduction

## What is information governance?

Information Governance is the system of controls (policies, processes, systems etc.) by which an organisation ensures that it meets its legal, policy and moral obligations in relation to the processing of information.

## Importance of information governance

Healthwatch Richmond holds and has access to sensitive information including the experiences of people who use services, correspondence with providers of care and their commissioners and regulators; commercially sensitive information, information from strategic partners about regulatory activity and other actions to protect people from harm and improve the quality of services.

Loss, misuse or mishandling of this information creates a direct risk to the privacy, dignity, rights and welfare of people who use services and may significantly damage the effectiveness of Healthwatch Richmond. It is particularly important to maintain public trust in the confidentiality and security of their personal information within the wider health and social care system. Loss of this trust may significantly impact upon the effectiveness of the health and social care sectors.

## Information Governance Framework and key roles

Healthwatch Richmond LTD is a company limited by guarantee and registered charity and the Data Controller for the purposes of Healthwatch Richmond. Because the Contract Data will revert to London Borough of Richmond upon Thames at the end of the contract, they are also a controller of the data.

As the Data Controller, Healthwatch Richmond will consult London Borough or Richmond upon Thames where there are significant variations in our practices that require decision making on matters of information management, information security, information risk management, legal compliance with information law, information sharing and the organisation’s statutory responsibilities under the Freedom of Information Act 2000, the Data Protection Act 1998, and other relevant legislation.

# Confidentiality

Information about individuals, third part organisations or Healthwatch Richmond that is not already in the public domain should usually be considered to be confidential. Confidential information may or may not be recorded and can include:

1. Information about Healthwatch Richmond: for example, its plans or finances
2. Information about third party organisations not already in the public domain
3. Information about individuals (for example, clients, volunteers and staff), whether recorded or otherwise

Confidential information must not be disclosed outside of Healthwatch Richmond whether verbally or in writing except in certain circumstances or unless we have a legal obligation or consent to disclose it, ideally in writing.

To guard against potential breaches of confidentiality information should only be sought from individuals if it is in their or the public for us to do so, i.e. to enable a better service delivery, and wherever possible information will be collected anonymously.

## Importance of confidentiality.

Some information held by Healthwatch Richmond carries the risk of adverse or damaging effects if disclosed. Most obviously, private information about individual people carries the risk of affecting their privacy, dignity, safety or welfare if disclosed. The handling of this type of information is covered in *“Using personal data and confidential personal information”*, page of this policy.

However, it is important to remember that other types of information may be confidential in nature too:

* Releasing information about a care provider may have a significant commercial impact upon their business.
* Information about planned or ongoing regulatory activity could prejudice the effectiveness of that activity.
* Information about local or national policy development or the management of Healthwatch Richmond or its stakeholders may pre-empt official announcements with damaging effect.

Whenever handling information, you should be mindful of whether the information is confidential in nature. Where appropriate, confidential information should be marked as such, and should always be handled with care.

We are still able to collect, use and share confidential information, but we should only do so with appropriate consideration, and where we are satisfied that our actions are lawful and in the public interest.

## Legal requirements

In some cases, Healthwatch Richmond will be covered by legal requirements of confidentiality. Our legal responsibility to protect information about people is covered in *“Using personal data and confidential personal information”*, page . Where Healthwatch Richmond has received information of a confidential nature (i.e. where disclosure has the potential to cause some damage or harm) in circumstances where it is reasonable to expect that we would protect that confidentiality (whether or not this has been explicitly agreed), we will be subject to the common law duty of confidentiality.

Whether there is a specific prohibition on disclosure or where the general common law duty of confidentiality applies, we may still have a legal basis to disclose information – but we must still exercise care in protecting the information and making these decisions.

This is covered further in, *“Information Sharing”*, page of this policy.

# Knowledge and Information Management

## Importance of records management

Records provide vital evidence of business decisions, activities and transactions. They are also essential in ensuring that Healthwatch Richmond meets legislative and regulatory requirements.

The key benefits for supporting Healthwatch Richmond in this are that records are:

* Captured and stored in the right place.
* Authentic so are confident that records are accurate.
* Accessible in a timely way, by those who need or have a right to see them.
* Protected from unauthorised deletion, changes or access.
* Disposed of appropriately once they are no longer required.

Primary records should be:

* Held in electronic format on our secure drive (or in the appropriate a paper filing systems for HR and financial records)
* Permissions to view and edit should be given to appropriate personnel (i.e. those who may have a legitimate need to access them in your absence), or restricted from those who should not have access to them
* Named and filed in a logical and consistent manner

## E-mail

Each member of staff is assigned an email account. This is not to be used as the primary storage location for records.

All records required for business purposes must be held in on the shared drive to ensure that they remain accessible.

## Retention of records

All records used, received or created by Healthwatch Richmond have a retention period assigned that meets legislative and business requirements.

Once this period ends, records must be either transferred for permanent storage or destroyed in a way appropriate to their content and storage format. This applies to all records whether electronic or physical (such as paper records).

| **Retention of Records in Healthwatch Richmond** | |
| --- | --- |
| **Employment** | |
| In general the staff records (including those of volunteers) should be retained for **6 years after the end of employment**, but need only contain sufficient information in order to provide a reference (e.g. training and disciplinary records). Copies of any reference given should be retained for 6 years after the reference request. Director’s files should be retained for 6 years. | |
| Application form | Duration of employment, destroy when employment ends |
| References received | Duration of employment, destroy when employment ends |
| Sickness and maternity records | 6 years from end of employment |
| Annual leave records | 6 years from end of employment |
| Unpaid leave/special leave records | 6 years from end of employment |
| Records relating to an injury or accident at work | 12 years |
| References given/information to enable a reference to be provided | 6 years from end of employment |
| Recruitment and selection material (unsuccessful candidates) | 2 years after recruitment is finalised |
| Disciplinary records | 6 years after employment has ended |
| Statutory Maternity Pay records, calculations and certificates | Retain while employed and for seven years after employment has ended |
| Redundancy details, calculation of payments and refunds | Seven years from date of redundancy |
| **Note:** if an allegation has been made about the member of staff, volunteer or trustee the staff record should be retained until they reach the normal retirement age or for 10 years, if that is longer. E.g. around Safeguarding. | |
|
| **Record of Comments and other evidence, e.g. observations, interviews, enter and view notes.** | |
| Comments recorded on internal databases | Retain in line with local policy |
| Any paper based comments recorded on the database. | 1 year (This is in case there is a query regarding an entry on the database) |
| Comments and or other evidence that have **not** been recorded on the database. | Retain in line with local policy |
|
| Signed consent forms | Destroy in line with above |
| **DBS checks** | |
| Record disclosure reference no. and date of check and return to the volunteer or staff member. | |
| Record of Concern Forms (ROCA) | |
| All ROCAs and related information should be kept for 10 years. If the record relates to children and young people the record must be kept till they are 21 years old before destroying. | |
| **Financial Records** | |
| Financial records | 6 years (public funded Companies) |
| Income tax and NI returns, income tax records and correspondence with HMRC | Not less than 3 years after the end of the financial year to which they relate |
| Payroll records (also overtime, bonuses, expenses) | 10 years |
| Pension contribution records | 6 years |
| Pension Scheme Investment Policies | 12 years from any benefit payable under the policy |
| **Corporate** | |
| Employers Liability Certificate | 40 years |
| Insurance policies | Permanently |
| Certificate of Incorporation | Permanently |
| Minutes of Board of Trustees | Permanently |
| Memorandum of Association | Original to be kept permanently |
| Articles of Association | Original to be kept permanently |
| Variations to the Governing Documents | Original to be kept permanently |
| Statutory Registers | Permanently |
| Membership records | 20 years from commencement of membership register |
| Rental or Hire Purchase Agreements | 6 years after expiry |
| **Others** | |
| Deeds of Title | Permanently |
| Leases | 12 years after lease has expired |
| Accident books | 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). |
| Health and Safety Policy Documents | Retain until superseded |
| Assessment of Risks under Health and Safety Legislation | Retain until superseded |
| **Contact Details** | |
| Paper forms | Upload to electronic system and destroy once it is confirmed that the contact details have been correctly uploaded (i.e. email sent and does not bounce). |
| Mailing lists | Retain until unsubscribed, notified of change or cleaned due to non-receipt of emails |
| Google Contacts (Day to day contact details and emails) | Retain until we receive a request to delete or are notified of a change of contact details |
| Postal contacts | Retain until we receive a request to delete. |

## Accessing records

For access to restricted areas staff must obtain authorisation from the Asset Owner.

Whether restricted or not, you must only access Healthwatch Richmond’s records as authorised and required for the exercise of your role.

# Information Security

Records stored on the Drive are protected by encryption and 2 sign in security with passwords having to exceed a minimum level of security.

Passwords protect the other systems that we use and these should always have comparative levels of security where possible.

The loss of any device that has been used to access this system or used for 2-step sign in must be reported immediately to the Chief Officer so that the system can be secured.

Logs of activity are made on all systems where possible and any unusual or unexpected activity must be reported to the Chief Officer who will secure the systems by resetting the passwords.

In the absence of the Chief Officer you must make every attempt to reset passwords of accounts that may have been compromised.

Our IT contractors can be contacted to provide assistance if required.

# Using personal data and confidential personal information

Personal data (and only personal data – confidential or otherwise) is subject to the Data Protection Act 2018.

All personal data is excluded from the Freedom of Information Act and associated.

## What is personal data

Personal data is defined under section 1 of the Data Protection Act 2018, it is information that relates to and identifies a living person, either on its own or when combined with other information we hold (or which is likely to come into our possession). Some personal data - such as information about a person’s ethnicity, religion, sexuality or sexual life, trade union membership, physical or mental health, or about alleged offences or prosecution – is defined as ‘sensitive personal data’ and is subject to greater legal protection.

## What is confidential personal information

Confidential personal information is defined under section 76 of the Health and Social Care Act 2008. It is personal data that has been obtained by Healthwatch Richmond in circumstances requiring it to be held in confidence. This could mean that there was an explicit agreement of confidentiality when information was provided to Healthwatch, or that a reasonable person would have considered that a duty of confidentiality was implied.

# Legal requirements and obligations

The Data Protection Act provides a set of Principles that must be followed when ‘processing’ (holding, obtaining, handling, using, sharing, altering, disposing of) personal data. The Health and Social Care Act 2008 creates a specific offence of disclosing confidential personal information except in defined circumstances.

## Fair processing

The most fundamental requirement of Data Protection compliance is ‘fair processing’. A key element of fair processing is a ‘no surprises’ approach where people are informed of who has their personal data, how they will use it and why. Processing someone’s personal data in a way that would be a surprise to a reasonable person is unlikely to be fair, and would therefore be unlawful. This creates an obligation to tell people, at the point where you collect their information, how and why you will use it. If there are elements of your intended use that are optional, the person should be told this and given an easy way to exercise choice. Where personal data is being collected via a third party, reasonable steps should be taken to communicate this information back to the ‘data subject’.

## Lawful processing

Processing of personal data must also be ‘lawful’. This requires that all of the Data Protection Principles must be met, the rights of individuals under the Act (e.g. the right to see what information we hold about them, to correct inaccurate information, and the right to object to the processing of information in ways which are damaging to them) must be complied with, and we must process personal data in accordance with other laws (such as the Human Rights Act 1998, which requires that any intrusion upon personal privacy must be justified and proportionate).

## Conditions for processing personal data

Personal data may only be processed where a condition under schedule 2 of the DPA is met. Sensitive personal data (information about a person’s racial or ethnic origin, political opinions, religious (or similar) beliefs, trade union membership, physical or mental health, sexual life, or relating to offences, alleged offences or prosecution) may only be processed where a condition under schedule 3 of the DPA is also met.

Our [Data Asset Register](https://www.healthwatchrichmond.co.uk/information-asset-register) sets out the lawful basis for our processing of data.

## Necessity Test

The necessity test is the decision making process designed to assist in reaching lawful decisions on obtaining, using and sharing confidential personal information/data.

The person considering the disclosure should understand what ‘legitimate purpose’ they are seeking to achieve by the proposed disclosure.

They should satisfy themselves that the intended action will be fair and meet a schedule 2 (and, for sensitive personal data, also a schedule 3) condition.

Then they should consider the two-step test:

STEP 1: Is the disclosure a necessary step in achieving this outcome?

If the outcome could reasonably be achieved, in an efficient and effective manner and within the available resources, by other means, then personal data should not be shared. For example, could anonymised or aggregated data be used instead? This step should include consideration of whether the minimum personal data required to achieve the purpose is being shared. We should not share more personal data than necessary.

STEP 2: Is the proposed disclosure proportionate?

Consideration should be given here to the likely impact upon the privacy and interests of the data subject (including any objections they have raised) and these should be balanced against the anticipated public interest to be served by disclosure.

In short, having considered the necessity test, the person should be satisfied that they would be able to explain and justify their actions if challenged.

## Anonymisation and pseudonymisation

Wherever possible, anonymised or pseudonomised data should be used instead of personal data / confidential personal information. Data of this type can be more freely used or shared, and its use minimises the risk to the privacy and dignity of individuals.

Anonymised data is information from which it is not possible to identify individuals – for example, aggregated data showing statistical information about large numbers of people.

Pseudonymised data is information where the identities of individuals are concealed, but where re-identification is possible – for example, narrative information about a person’s care where their name is replaced with a pseudonym such as ‘patient A’.

Care should be taken as simply removing names, addresses etc. does not always guarantee that individuals cannot be identified.

Advice should be sought if in doubt.

## Authorisation to use PD/CPI and PIA

When considering new ways of using information – for example, planning the introduction of new systems, processes or policies – consideration should be given as to whether the proposed changes will involve changes to the way in which personal data or other confidential information will be obtained, used, stored or shared.

Where this is likely to be the case, appropriate authorisation must be sought from the Chief Officer in the first instance and if necessary from the DPO appointed by London Borough if Richmond upon Thames.

Privacy impact assessments are a structured way to assess the likely risks to personal privacy arising from changes, and for putting appropriate measures in place to mitigate those risks.

# Information Sharing

## Why we share information

The appropriate and effective sharing of information can play a vital role in protecting people from harm, improving services and in facilitating the exercise of strategic partners such as NHS, Richmond Council, Healthwatch England and CQC.

## Legal requirements

Personal data must only be shared where it is fair and lawful to do so.

Consideration should be given to whether data subjects would reasonably have expected their personal data to be shared by Healthwatch Richmond. In making this assessment, consideration should be given to any information previously provided to the data subject, any discussions with them, any indication they have given about how they wish or expect their data to be used, and publicly available information materials about uses of information.

Consideration may also be given to what information the data subject themselves has put into the public domain. Where they have made their own information public, then it is more likely to be fair to share that information – however, care should be taken in differentiating between information that the person has made public and information that they may reasonably expect to be maintained in confidence.

Where it is considered that the data subject would not reasonably expect their information to be shared, they should be contacted and their consent sought for the disclosure.

Where it is not appropriate or possible to do this, consideration should be given to whether there is another lawful basis which would permit a disclosure which would otherwise be unfair. The only exemptions which are likely to apply are:

* Where the disclosure is necessary for the prevention or detection of crime, or the prosecution of offenders. This may apply where the disclosure is considered to be necessary for regulators to investigate allegations of serious breaches of regulations or offences relating to registered activities.
* Disclosures which are necessary in connection with legal proceedings, proposed legal proceedings, or for the purpose of obtaining legal advice.

In other cases, exceptional circumstances may permit the sharing of information. Most notably, a disclosure that is considered necessary to protect a person from significant risk of serious harm would be permissible.

## Making decisions to share information

Decisions on sharing personal data should be made using the ‘necessity test’ (see above).

Confidential medical information about identifiable people should only be shared without consent where there is a very high public interest in doing so.

Decisions on sharing other kinds of information should take into account the potential impact of disclosure and the possible prejudice or damage that may be caused.

## Authorisation

You should only share information if you are authorised to do so as part of your role, or where you have authorisation to do so from the Chief officer or DPO.

# Access to Information

We are the Data Controller in respect of Healthwatch Richmond and must ensure that Individuals are able to exercise their rights under the new data protection laws (General Data Protection Regulation (GDPR) 2018 and Data Protection Act 2018) subject to certain exemptions.

The Data Protection Act creates the following rights that we must respect:

1. [Right to be informed](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/)
2. [Right of access](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/)
3. [Right to rectification](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/)
4. [Right to erasure](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/)
5. [Right to restrict processing](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/)
6. [Right to data portability](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/)
7. [Right to object](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/)
8. [Rights related to automated decision making including profiling](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/)

Healthwatch is named on the Freedom of Information Act and is required to respond to all requests for information within one month. There are significant [exemptions](http://www.legislation.gov.uk/ukpga/2000/36/part/II) to this, some of which are of particular importance to us including:

* accessible to applicant by other means
* intended for future publication
* personally identifiable

## What to do if you receive a request

If you receive a request whether in relation to the Freedom of Information Act or Data Protection Act whether written or otherwise it should be passed immediately to the Chief Officer as we have 20 days to deal with FOI and 1 month for DPA requests.

1. We will consider each request in light of legal requirements to identify what must be done.
2. In respect of Data Protection Rights we will satisfy ourselves that the individual requesting the data is the data subject or has their consent.
3. We will review our data asset register to identify all databases that might contain relevant information associated with the request.
4. All storage systems/locations identified by the action plan will be searched to identify all relevant data.
5. Each item of data will be considered in relation to our legal reasons for processing and retaining records.
   * The Chief Officer will decide whether to give access to, amended or deleted data according to guidance from the ICO, exemptions from the Data protection Act (see Appendix 1) or [exemptions from the Freedom of Information Act](http://www.legislation.gov.uk/ukpga/2000/36/part/II). Our response will explain our reasons for refusing a request or part of a request.
6. We must respond within:
   * 1 month of receiving a request under the Data Protection Act
   * 20 working days of receiving a FOI Request.

## Sign-off and decision making

All responses to requests for information regarding Healthwatch Richmond are signed off by the Chief Officer in line with the Authorising Public Statements Policy.

## Disclosure of information about you

You should be aware that information about your role, professional decisions and actions may be disclosed in response to requests. Generally speaking, information of a personal nature will not be disclosed.

The more senior and public facing your role, the more likely it is that information about you may have to be disclosed. Where potentially sensitive or confidential information about you is being considered for disclosure, you will be consulted.

# Support and guidance

In the first instance approach the Chief Officer. In his/her absence contact an Officer of the Board (Chair, Healthwatch Committee Chair, Audit Committee Chair or Treasurer).

The Data Protection Officer (where appointed) will provide advice to the Chief Officer.

**EXEMPTIONS TO BE USED WHEN DENYING A SAR**

**SUMMARY OF EXEMPTIONS TO THE DPA 2018 USED BY COUNCILS**

**(see GDPR ref: at Article 6(3) and 23(1) of the GDPR 2018)**

See the DPA 2018 Act for full wording, the DPO is available for further advice

| **DPA 2018 exemption** | **New DPA 2018 reference** | **What does it apply to** | **DPA98 Ref** |
| --- | --- | --- | --- |
| GDPR provisions to be restricted: ‘the listed GDPR provisions’. | Schedule 2: Part 1: Paragraph 1 | Listed provisions within the GDPR which may be restricted   * Personal data collected from the data subject: information to be provided – Article 13 * Personal data collected other than from data subject: information to be provided – Article 14 * Confirmation of processing, access to data and safeguards for third country transfers – Art 15 * Right to rectification – Article 16 * Right to erasure – Article 17 * Restriction of processing – Article 18 * Notification obligation regarding rectification or erasure of personal data or restriction in processing – Article 19 * Right to data portability – Article 20 * Objections to processing – Article 21 * General principles (fair, specific, limitation, adequate, accurate, secure) – Art 5 |  |
| Crime & Taxation: general | Schedule 2: Part 1: Paragraph 2 | Informing data subject of data breach where data has been processed for the prevention and detection of crime, the apprehension or prosecution of offenders of the assessment or collection of a tax or duty or an imposition of a similar nature | S 29 |
| Crime & Taxation: risk assessment systems | Schedule 2: Part 1: Paragraph 3 | Where personal data is processed for crime and taxation purposes by a data controller who is a public body and the restrictions are necessary for the smooth running of a risk assessment system. It restricts a more limited set of GDPR provisions. | S 29 |
| Immigration | Schedule 2: Part 1: Paragraph 4 | Restricts the application of the listed GDPR provisions to person data processed for the purposes of the maintenance of effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control, to extent that the application of those provisions would be likely to prejudice those purposes. | None, new |
| Legal Proceedings | Schedule 2: Part 1: Para 5 | Restricts the application of the listed GDPR provisions to the processing of data protection where the data controller is obliged, under an enactment, to disclose personal data to the public, to the extent the application of those provisions would prevent compliance with that obligation. | S 34  S 35 |
| **DPA 2018 exemption** | **New DPA 2018 reference** | **What does it apply to** | **DPA98 ref** |
| GDPR provisions to be restricted: ‘the listed GDPR provisions’. | Schedule 2: Part 2: Paragraph 6 | Listed provisions within the GDPR which may be restricted   * Personal data collected from the data subject: information to be provided – Article 13 * Personal data collected other than from data subject: information to be provided – Ar14 * Confirmation of processing, access to data, safeguards for 3rd country transfers – A 15 * Right to rectification – Article 16 * Right to erasure – Article 17 * Restriction of processing – Article 18 * Notification obligation regarding rectification or erasure of personal data or restriction in processing – Article 19 * Right to data portability – Article 20 * Objections to processing – Article 21 * General principles (fair, specific, limitation, adequate, accurate, secure) – Art 5 |  |
| Function designed to protect the public | Schedule 2: Part 2: Paragraph 7 | Restricts the application of the listed GDPR provisions to personal data processed for the purposes of discharging the functions concerned with the protection of members of the public, charities and fair competition in business. Includes financial loss due to dishonesty, malpractice, unfitness, incompetence, protect charities or community interest companies against mis-management, protect health and safety at work, failures in services provided by public bodies. | S 31 |
| Audit Functions | Schedule 2: Part 2: Paragraph 8 | Restricts the application of the listed GDPR provisions to personal data processed for the purposes of discharging statutory functions. | S 31 |
| Regulatory functions relating to legal services, health service children services | Schedule 2: Part 2: Paragraph 10 | Restricts the application of the listed GDPR provisions to personal data processed for the purpose of discharging regulatory functions relating to legal services, the health service and children’s service to the extent that the application of those provisions would be likely too prejudice the proper discharge of the function. | S 31 |
| Regulatory functions of certain other persons | Schedule 2: Part 2: Paragraph 11 | Restricts the application of the listed GDPR provisions to personal data processed in certain other public bodies for the purpose of discharging their statutory functions. These other bodies include The Commissioner, various Pensions Regulators, Monitoring officers of a relevant authority, Financial Regulators, The Charity Commission. | S 31 |
| Judicial issues | Schedule 2: Part 2: Paragraph 14/15 | Restricts the application of the listed GDPR provisions relating to all other personal data to the extent the application of those provisions would be likely to prejudice judicial independence or proceedings. This ensures that the administration of justice is not undermined by GDPR. | S 37 |
| Crwn Hons, dig’ties, appointments | Schedule 2: Part 2: Para 15 | Restricts the application of the listed GDPR provisions to personal data processed for the purposes of conferring Crown Honours, or for assessing suitability for offices. | S 37 |
| **DPA 2018 exemption** | **New DPA 2018 reference** | **What does it apply to** | **DPA98 ref** |
| Protection of the rights of others (16)  Assumption of reasonableness for health workers, social workers and education workers (17) | Schedule 2: Part 3: Paragraph 16 & 17 | Does not oblige a controller to disclose information to the data subject to the extent that the doing so would involve disclosing information relating to another individual who can be identified from the information. Except where the other individual has consented; or it is reasonable in all circumstances to comply with the request without the individual’s consent. | S 7  S 8 |
| **DPA 2018 exemption** | **New DPA 2018 reference** | **What does it apply to** | **DPA98 ref** |
| GDPR provisions to be restricted: ‘the listed GDPR provisions’. | Schedule 2: Part 4: Paragraph 18 | Listed provisions within the GDPR which may be restricted   * Personal data collected from the data subject: information to be provided – Article 13 * Personal data collected other than from data subject: information to be provided – Article 14 * Confirmation of processing, access to data and safeguards for third country transfers – Art 15 * General principles (fair, specific, limitation, adequate, accurate, secure) – Article 5 |  |
| Legal Professional Privilege | Schedule 2: Part 4: Paragraph 19 | Restricts the application of the listed GDPR provisions for Part 4, as above, to personal data that consists of information over which a claim to LLP could be maintained in legal proceedings or information covered by a duty of confidentiality owed by a professional legal adviser to a client. | S 37 |
| Self-Incrimination | Schedule 2: Part 4: Paragraph 20 | Restricts the obligation to comply with the listed GDPR provisions for Part 4, as above, to the extent that compliance will result in self-incrimination i.e. by revealing evidence of the commission of an offence, expose the person to proceedings for that offence. It also provides that information disclosed by a person under SAR is not admissible against the person in proceeding for an offence under ICO and enforcement. | S 37 |
| Corporate Finance | Schedule 2: Part 4: Paragraph 21 | Restricts the application of the listed GDPR provisions for Part 4, as above, to personal data processed for the purposes of, or in connection with, a corporate finance to the extent that one of the application of the listed GDPR provisions would be likely to affect the price of an instrument or have an effect on a person as to whether deciding to deal with an instrument and therefore have an effect on the business activity and have a prejudicial effect on the orderly functioning of financial markets or the economy. | D 37 |
| Management Forecasts | Schedule 2: Part 4: Paragraph 22 | Restricts the application of the listed GDPR provisions for Part 4, as above, to personal data processed for management forecasting or management planning purposes, to the extent that the application of those provisions would prejudice the conduct of the business or activity concerned. | S 37 |
| Negotiations | Schedule 2: Part 4: Paragraph 23 | Restricts the application of the listed GDPR provisions for Part 4, as above, to personal data that consists of a data controllers record of their intentions in relation to any negotiations with the data subject, to the extent that the applications of those provisions likely to prejudice the negotiation. | S 37 |
| Confidential References | Schedule 2: Part 4: Paragraph 24 | Restricts the application of the listed GDPR provisions for Part 4, as above, to personal data consisting of a reference given (or to be given) (received) in confidence for education, employment, placement as a volunteer and the provision by the data subject of any service. | S 37 |
| Exam scripts and exam marks | Schedule 2: Part 4: Paragraph 25 | Restricts the application of the listed GDPR provisions for Part 4, as above, to personal data consists of information recorded by candidates. | S 37 |
| **DPA 2018 exemption** | **New DPA 2018 reference** | **What does it apply to** | **DPA98 ref** |
| Journalistic, academic, artistic or literary purpose (known as ‘special purposes’) | Schedule 2: Part 5: Paragraph 26 | Listed provisions with the GDPR’s which may be restricted.   * Personal data collected from the data subject: information to be provided – Article 13 * Personal data collected other than from data subject: information to be provided – Article 14 * Confirmation of processing, access to data and safeguards for third country transfers – Art 15 * Right to rectification – Article 16 * Right to erasure – Article 17 * Restriction of processing – Article 18 * Notification obligation regarding rectification or erasure of personal data or restriction in processing – Article 19 * Right to data portability – Article 20 * Objections to processing – Article 21 * All principles except the security and accountability – Article 5 * The lawful bases – Article 6 * The conditions for consent – Article 7 * Children’s consent – Article 8 * The conditions for processing special categories of personal data - Article 9 * Data relating to criminal convictions and offences – Article 10 * Processing not requiring identification– Article 11 * Right to be informed * the communication of personal data breaches to individuals – Article 34 * consultation with the ICO for high risk processing – Article 36 * international transfers of personal data – Article 44 * cooperation and consistency between supervisory authorities – Articles 60--67   The listed provisions do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purposes. |  |
|  |
| **DPA 2018 exemption** | **New DPA 2018 reference** | **What does it apply to** | **DPA98 ref** |
| Research and statistics | Schedule 2: Part 6: Paragraph 27 | Listed provisions within the GDPR which may be restricted   * Confirmation of processing, access to data and safeguards for third country transfers – Article 15 * Right to rectification – Article 16 * Restriction of processing – Article 18 * Objections to processing – Article 21   The listed provisions do not apply to the extent that the controller reasonably believes that the application of those provisions would prevent or seriously impair the achievement of the purposes in question. | S 33 |
| Archiving in the public interest | Schedule 2: Part 6: Paragraph 28 | Listed provisions with the GDPR’s which may be restricted.   * Confirmation of processing, access to data and safeguards for third country transfers – Art 15 * Right to rectification – Article 16 * Restriction of processing – Article 18 * Notification obligation regarding rectification or erasure of personal data or restriction in processing – Article 19 * Right to data portability – Article 20 * Objections to processing – Article 21   The listed provisions do not apply to personal data processed for archiving purposes in the public interest to the extent that that the application of those provisions would seriously prevent impair the achievement of those purposes. | S 37 |
| **DPA 2018 exemption** | **New DPA 2018 reference** | **What does it apply to** | **DPA98 ref** |
| Exemptions from the GDPR: Health, social work, education and child abuse. | Schedule 3: Part 1: Paragraph 1 | Listed provisions within the GDPR which may be restricted   * Personal data collected from the data subject: information to be provided – Article 13 * Personal data collected other than from data subject: information to be provided – Article 14 * Confirmation of processing, access to data and safeguards for third country transfers – Art 15 * Right to rectification – Article 16 * Right to erasure – Article 17 * Restriction of processing – Article 18 * Right to data portability – Article 20 * Objections to processing – Article 21 * General principles (fair, specific, limitation, adequate, accurate, secure) – Article 5 |  |
| Health Data:  Definitions | Schedule 3: Part 2 |  |  |
| Health Data:  data processed by a court | Schedule 3: Part 2: Paragraph 3 | Restricts the application of the listed GDPR provisions to personal data concerning health if it is processed by a court, consists of information supplied in a report to the court during the course of the proceedings. | S 30 |
| Health Data: data subject’s expectations and wishes | Schedule 3: Part 2: Paragraph 4 | Restricts the application of the listed GDPR provisions to personal data to the extent that complying with the request would disclose information—  (a)which was provided by the data subject in the expectation that it would not be disclosed to the person making the request,  (b)which was obtained as a result of any examination or investigation to which the data subject consented in the expectation that the information would not be so disclosed, or  (c)which the data subject has expressly indicated should not be so disclosed.  The exemptions under sub-paragraph (a) and (b) do not apply if the data subject has expressly indicated that he or she no longer has the expectation mentioned there. | S 30 |
| Health Data: serious harm | Schedule 3: Part 2: Paragraph 5 | Restricts the application of the listed GDPR provisions to personal data where “serious harm test” is met with respect to data concerning health if the application of Article 15 of the GDPR to the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual. | S 30 |
| Health Data:  Restriction of Article 15 of the GDPR: prior opinion of appropriate health professional | Schedule 3: Part 2: Paragraph 6 | Restricts the application of the listed GDPR provisions to personal data where “the appropriate health professional”, in relation to a question as to whether the serious harm test is met with respect to data concerning health, means—  (a) the health professional who is currently or was most recently responsible for the diagnosis, care or treatment of the data subject in connection with the matters to which the data relates,  (b)where there is more than one such health professional, the health professional who is the most suitable to provide an opinion on the question, or  (c)a health professional who has the necessary experience and qualifications to provide an opinion on the question. | S 30 |
| **DPA 2018 exemption** | **New DPA 2018 reference** | **What does it apply to** | **DPA98 ref** |
| GDPR provisions to be restricted | Schedule 3: Part 3 | Listed provisions within the GDPR which may be restricted   * Personal data collected from the data subject: information to be provided – Article 13 * Personal data collected other than from data subject: information to be provided – Article 14 * Confirmation of processing, access to data and safeguards for third country transfers – Art 15 * Right to rectification – Article 16 * Right to erasure – Article 17 * Restriction of processing – Article 18 * Right to data portability – Article 20 * Objections to processing – Article 21 * General principles (fair, specific, limitation, adequate, accurate, secure) – Article 5 |  |
| Social Work Data:  data processed by a court | Schedule 3: Part 3: Paragraph 9 | Restricts the application of the listed GDPR provisions to personal data that is not health or education data if it is processed by a court, consists of information supplied in a report to the court during the course of the proceedings. | S 30 |
| Social Work Data:  data subject’s expectations and wishes | Schedule 3: Part 3: Paragraph 10 | The listed GDPR provisions do not apply to social work data to the extent that complying with the request would disclose information—  (a)which was provided by the data subject in the expectation that it would not be disclosed to the person making the request,  (b)which was obtained as a result of any examination or investigation to which the data subject consented in the expectation that the information would not be so disclosed, or  (c)which the data subject has expressly indicated should not be so disclosed.  The exemptions under sub-paragraph (a) and (b) do not apply if the data subject has expressly indicated that he or she no longer has the expectation mentioned there. | S 30 |
| Social Work data:  Exemption from Article 15 of the GDPR: serious harm | Schedule 3: Part 3: Paragraph 11 | For the purposes of this Part of this Schedule, the “serious harm test” is met with respect to social work data if the application of Article 15 of the GDPR to the data would be likely to prejudice carrying out social work, because it would be likely to cause serious harm to the physical or mental health of the data subject or another individual. | S 30 |
| Social Work Data:  Restriction of Article 15 of the GDPR: prior opinion of Principle Reporter | Schedule 3: Part 3: Paragraph 12 | Where the data—  (i)originated from or was supplied by the Principal Reporter acting in pursuance of the Principal Reporter’s statutory duties, and  (ii)is not data which the data subject is entitled to receive from the Principal Reporter.  The controller must inform the Principal Reporter of the fact that the question has arisen before the end of the period of 14 days beginning when the question arises.  (3)Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) do not permit the controller to disclose the data to the data subject unless the Principal Reporter has informed the controller that, in the opinion of the Principal Reporter, the serious harm test is not met with respect to the data. to the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual. |  |
| GDPR provisions to be restricted.  Education Data | Schedule 3: Part 4 | Listed provisions within the GDPR which may be restricted   * Personal data collected from the data subject: information to be provided – Article 13 * Personal data collected other than from data subject: information to be provided – Article 14 * Confirmation of processing, access to data and safeguards for third country transfers – Art 15 * Right to rectification – Article 16 * Right to erasure – Article 17 * Restriction of processing – Article 18 * Notification obligation regarding rectification or erasure of personal data or restriction in processing – Article 19 * Right to data portability – Article 20 * Objections to processing – Article 21 * General principles (fair, specific, limitation, adequate, accurate, secure) – Article 5 |  |
| Education Data:  Exemptions from the listed GDPR provisions: data processed by a court | Schedule 3: Part 4: Paragraph 18 | The listed GDPR provisions do not apply to data that is not education data or data concerning health if—  (a)it is processed by a court,  (b)it consists of information supplied in a report or other evidence given to the court in the course of proceedings to which rules listed in subparagraph (2) apply, and  (c)in accordance with any of those rules, the data may be withheld by the court in whole or in part from the data subject | S 30 |
| Education data:  Exemption from Article 15 of the GDPR: serious harm | Schedule 3: Part 4: Paragraph 19 | Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) do not apply to education data to the extent that the serious harm test is met with respect to the data. it would be likely to cause serious harm to the physical or mental health of the data subject or another individual. | S 30 |
| Education Data:  Restriction of Article 15 of the GDPR: prior opinion of Principle Reporter | Schedule 3: Part 4: Paragraph 20 | Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) do not permit the controller to disclose the data to the data subject unless the Principal Reporter has informed the controller that, in the opinion of the Principal Reporter, the serious harm test is not met with respect to the data. | S 30 |
| Child abuse data | Schedule 3: Part 5: Paragraph 21 | Where a request for child abuse data is made in exercise of a power conferred by an enactment or rule of law and—  (a)the data subject is an individual aged under 18 and the person making the request has parental responsibility for the data subject, or  (b)the data subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs.  Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers) do not apply to child abuse data to the extent that the application of that provision would not be in the best interests of the data subject.  “Child abuse data” is personal data consisting of information as to whether the data subject is or has been the subject of, or may be at risk of, child abuse.  For this purpose, “child abuse” includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of, an individual aged under 18 | NA – New` |