**KETTLESHULME ST JAMES CE (VA) PRIMARY SCHOOL**

**Subject Access Policy**

**and Procedure**

**Summer 2023**

**Review Date - Summer 2025**

**To be reviewed along with Data Protection Policy**

# Introduction

* 1. The purpose of this guidance document is to assist staff in identifying and dealing with requests for personal information about individuals. The guidance covers requests from individuals for information about themselves, requests made on behalf of individuals and requests from third parties for disclosure of information about individuals.
  2. Cheshire East Council holds a considerable amount of personal data about individuals including staff, elected members, contractors, service users and members of the public who have dealings with the Council. The information comes from a variety of sources, for example the individual themselves, other local authorities or government agencies, professionals or other individuals such as complainants. Personal information is also held in various forms including paper files, electronic records such as information systems and emails as well as photographs, CCTV footage, diaries, notebooks and audio recordings.
  3. The General Data Protection Regulation (GDPR) gives all individuals within the European Union the same set of rights with regards to how organisations deal with their personal data. These are listed in the GDPR in Articles 12 – 23. The Data Protection Act 2018 (DPA) underpins these rights and provides further detail and exemptions where necessary.

# **Right of Access**

* 1. Article 15 of GDPR gives individuals the right to see, and be provided with a copy of, personal information which organisations hold about them, subject to a limited number of exemptions. This is known as a Subject Access Request or Access to Records in social services terms. A person does not necessarily have the right to know what is recorded about someone else without proper authority.
  2. Personal data is information relating to a living individual who can be identified from that information (either on its own or along with other information held by the organisation).
  3. Individuals have a right to be:
* Told whether any personal data is being processed;
* Given a description of the personal data, the reasons it is being processed and whether it will be given to any other organisations or people;
* Given a copy of the personal data;
* Given details of the source of the data where this is available and where it does not identify a living individual; and
* Given details of their rights and how to make a complaint.
  1. Requests can be in any form. Requests in writing will be the most common; however a verbal request (by phone or in person) should be processed, subject to the same need to confirm the requester’s identity. A form is available, on both the website and Centranet, but this does not have to be used to make the request valid.
  2. To ensure personal information is not disclosed to someone not entitled to it, the Council has to be satisfied as to the identity of the person making the request and the identity of anyone making a request on their behalf. In a change from the previous legislation, in most circumstances we can NOT charge an administration fee. The exceptions to this are where the request is “manifestly unfounded or excessive”, in which case a reasonable fee can be charged. A request is manifestly unfounded when the individual making the request is not actually seeking the information being requested, but is instead seeking to harm the organisation by wasting time and administrative costs. A request is considered excessive in relation to its repetitive nature i.e. if someone is repeatedly requesting the same information. Please note that in both cases the burden of proof is on the Council to prove that a request meets one or both of these criteria and as such significant caution should be exercised before attempting to charge a data subject a fee for a request.
  3. See section 13 of this document for details of procedure to be followed.

# Right to Erasure

* 1. Article 17 of the GDPR gives individuals the right to have personal data erased. This is also known as the ‘right to be forgotten’.
  2. This is a new right under GDPR which was not included in the 1998 Act.
  3. This is not an absolute right and only applies in certain circumstances. Personal data will be erased on request only if one of the following applies:
* the personal data is no longer necessary for the purpose which you originally collected or processed it for;
* the basis for processing is “consent”, and the individual wishes to withdraw their consent;
* the data is being processed for the purpose of direct marketing;
* the data is being processed unlawfully;
* some other legal obligation

It is important to know the basis for which we are processing the data. You can find the reason that data is being processed on the council’s [Information Asset Register](https://opendata.cheshireeast.gov.uk/Council-and-Democracy/Information-Asset-Register-For-GDPR/ht96-pp6s/data) or the service’s privacy notice.

* 1. This right does not apply if the data is currently being processed while performing a task in the public interest or in the exercising of official powers. Therefore it will not apply to most council services.
  2. Please see Section 13 of this document for the procedure to follow when you identify such a request.

# Right to Object

* 1. Article 21 of the GDPR gives individuals the right to object to the processing of their data.
  2. Individuals have the absolute right to object to their data being used for direct marketing.
  3. If we are processing their information on the basis of a task carried out in the public interest (most of the services provided by Cheshire East Council) the individual may raise an objection to our continued use.
  4. The individual making the request must give reasons why they object to the processing of their data, these should be based on their personal circumstances. Additional weight should be given where damage or distress are being caused.
  5. Please follow the procedure in section 13 of this document for what to do with a request.
  6. Even where good reasons are given, if we feel we are processing the information with compelling legitimate grounds which override the interests of the individual, we can continue with the processing.
  7. In either case we should explain the outcome of our decision and any reasons for refusing. In this case we need to inform them of their right to complain to the ICO.

# **Requests by, or on behalf of, a child or young person under 18**

* 1. The data protection rights under GDPR extend to children and young people under 18 who understand what it means to exercise that right. While there is nothing in the GDPR or DPA to say how old a child might be to have sufficient understanding, the Information Commissioner’s Office guidance suggests the age of 12 as a guide. The relevant case worker, together with the Data Protection Officer, must decide whether the child/young person understands the nature of the request. If so, the request for access should be complied with.
  2. If the child or young person does not have sufficient understanding to make his/her own request, then a person with parental responsibility can make the request on the child’s behalf. This is usually a parent, but it could also be a legal guardian, and proof of parental responsibility must be provided.
  3. Birth mothers have automatic parental responsibility (unless it has been removed by order of the court). In most cases a copy of the child’s full birth certificate will be sufficient to prove parental responsibility of the mother. It is more difficult for a birth father to prove parental responsibility.
  4. If a father makes a request for his child’s records, a copy of one of the following documents will be required:
* The child’s full birth certificate – to acquire parental responsibility the father and mother must have registered the child’s birth together on or after 1 December 2003; or
* Marriage Certificate (a father who is married to the mother of their child at the time of birth automatically has parental responsibility); or
* Parental Responsibility Agreement entered into by birth parents; or
* A Court Order giving father parental responsibility

Alternatively, a father could provide signed permission from the child’s mother authorising the authority to disclose the child’s records to him.

* 1. Where the case worker considers that granting access to a parent is likely to result in significant harm to anyone or is not in the child’s best interests, access may be refused. The reasons for refusal must be recorded in writing and included in the child’s file. The parent may appeal to the Court or the Information Commissioner’s Office.

# Requests on behalf of a person lacking mental capacity

* 1. Any person over the age of 18 with a mental illness who has legal capacity, ie he/she understands the nature of the request, can make a subject access request.
  2. If a person lacks capacity to manage their affairs, someone acting under an order of the Court of Protection or acting within the terms of a registered Enduring Power of Attorney can request access on his/her behalf.

# Requests made through another person

* 1. If a person has capacity and if he/she has appointed an agent, for example a solicitor, friend or another member of the family, that person can make a valid request for access on behalf of the individual. Agents should provide evidence of their authority and confirm their identity and relationship to the individual. If satisfied that the individual has authorised the agent to make the request, the authority must treat the request as if it had been made by the individual. This also applies where a person is acting on another’s behalf under a general Power of Attorney.
  2. A person who is profoundly physically disabled may not be able to give written consent for an agent to make a request on their behalf. Where the person is unable to give written consent, as much assistance as possible should be given and a judgement made by the relevant case worker, with the Data Protection Officer, on whether the individual has given consent for an agent to act on their behalf.
  3. If there is any reason to believe that someone is falsely claiming to act on behalf of a person making a subject access request, this should be investigated before disclosing any information.

# Requests for Records of a Deceased Person

* 1. The GDPR and DPA apply only to data about living individuals; therefore data held about the deceased is not personal data as defined by the Act. However, even though the GDPR or DPA does not apply, there may still be issues of confidentiality surrounding access to records about the deceased. Any duty of confidence to the deceased goes beyond the grave and must be maintained, for example any statements made or recorded by the individual before they died for information not to be disclosed.
  2. General information about the deceased may be disclosed under the Freedom of Information Act 2000, but medical or health records may only be disclosed to the deceased’s personal representative and only then if there is no duty of confidentiality owed to the deceased. The personal representative can make an application for medical or health records through the Access to Health Records Act 1990 (AHRA). However, there is a clear distinction between "health records" and our "social care records" and that the 1990 Act does not give any right of access to social care records.
  3. Requests for information about the deceased should be forwarded to Compliance and Customer Relations who will advise how they should be dealt with.
  4. The deceased’s personal representative may not necessarily be the next of kin but is the person dealing with the deceased’s estate.
  5. As well as proof of identity, evidence of the requester’s relationship to the deceased and whether they are an executor of the estate is also required. A copy of a will or letter of probate will usually provide sufficient evidence.
  6. Depending on the number of copies having to be made and whether the records are only held in paper form, a charge may be made up to a maximum of £50. The timescale for responding to requests under the AHRA is 40 calendar days.

# Disclosure of information that includes details about another person

* 1. Responding to a subject access request may involve providing information that relates both to the requester and another individual (third party). The authority does not have to comply with a subject access request if it would mean disclosing information about a third party who can be identified from that information, except where
* The other individual has consented to the disclosure; or
* It is reasonable in all the circumstances to comply with the request without that individual’s consent.
  1. To decide what is reasonable in the circumstances, the following factors must be considered:
* Any duty of confidence owed to the other individual
* Any steps taken to seek their consent
* Whether the other individual is capable of giving consent
* Whether consent has been expressly refused
  1. The relevant case worker, with the Data Protection Officer, must make the decision on a case by case basis. There is no blanket policy of withholding third party information. The decision will involve balancing the data subject’s right of access against the other individual’s rights in respect of their own personal data. Consent from third parties should be sought where possible and if consent is not obtained, a decision must be made whether to disclose the information anyway. Obtaining consent may be particularly difficult when a request is received for access to very old files and the possibility of tracing other identified individuals is remote. If consent is not given, or cannot be sought, by the third party, the authority should still give as much information as possible without identifying that person.
  2. Schedule 2, Part 3, paragraph 16 of the DPA 2018 provides the relevant exemption regarding the protection of the rights of others.

# Redaction

* 1. Redaction is the process of removing third party personal data from the information being provided to the data subject. The disclosed information should show that information has been removed, ie use suitable software for electronic records. Avoid using a black marker as this is not an effective method of redaction. Do not use Tipp-ex as this does not clearly show where information has been removed. It can also appear messy if not dry properly when the document is copied and can stick to photocopier rollers causing expensive damage and marks on subsequent copies.
  2. If redaction is carried out using a black marker as the only method available, use single-sided copies to avoid black marker coming through to reverse and always photocopy or scan page again to prevent information being read through the marker. Please check redacted information cannot be read through the marker before sending out to the individual.
  3. If the document requiring redaction is in PDF format then some members of staff have access to Adobe Pro software allowing true electronic redaction. Do not attempt to redact electronic documents without the correct software as changes may be able to be reversed.
  4. In all cases, ensure original copy is retained to evidence what has been removed and to assist with any explanation or justification for the withheld information as necessary.

# Requests for Disclosure of Personal Data by Third Parties/Agencies

* 1. Cheshire East Council is the data controller of all personal data held and processed by the organisation. Decisions about disclosure rest entirely with the Council even where the information has been provided by a third party. However, any objections from third parties to disclosure must be taken into account and consent should be sought if appropriate.
  2. The most common requests for disclosure are from the police in relation to criminal investigations and solicitors pursuing legal proceedings on behalf of individuals. Requests can also be received from government agencies such as HM Revenue & Customs, Department for Work and Pensions, Child Support Agency, Home Office Border Agency and other local authorities.
  3. Schedule 2 of the Data Protection Act 2018 provides exemptions which allow disclosure of personal information in these circumstances (see paragraph 12).
  4. Court Orders must be complied with in all circumstances.

# Exemptions

12.1 There are a number of exemptions to processing personal data but the following are the most common exemptions used when dealing with requests for disclosure of information under the DPA 2018. Please note that exemptions are discretionary and not obligatory. If there are real concerns about disclosure of information, even if an exemption applies, the request can be refused and the requester will have to obtain a court order for disclosure. Such concerns should be discussed with the Data Protection Officer.

## Schedule 2 Part 1 Section 2– Crime and Taxation

* + 1. Requests for disclosure of personal data for certain purposes to do with criminal justice or the taxation system are exempt from the non-disclosure provisions of the DPA. This means information requested for the purpose of…
* the prevention or detection of crime;
* the apprehension or prosecution of offenders; and
* the assessment or collection of tax or duty
  + 1. Personal data can be disclosed where non-disclosure would be likely to prejudice the crime and taxation purposes. Judgement is required on a case by case basis to determine whether or not the exemption applies.
    2. Personal data processed for crime and taxation purposes is also exempt from the subject access provisions where disclosure would be likely to prejudice those purposes.

## Schedule 2 Part 1 Section 5 – Legal Proceedings

* + 1. Personal data is exempt from the non-disclosure provisions where the disclosure of the data is necessary:
* for, or in connection with, any legal proceedings (including prospective legal proceedings);
* for obtaining legal advice; or
* for establishing, exercising or defending legal rights.
  + 1. We do not have to disclose personal data in response to a request from a third party simply because this exemption applies. Decisions to disclose should be made on a case by case basis and the exemption should only be applied if satisfied that the disclosure falls within the scope of the exemption.

## Schedule 3 Parts 2, 3 and 4 – Health, Education and Social Work

* + 1. Personal data relating to an individual’s physical or mental health is exempt from the subject access provisions in certain circumstances and only if granting subject access would be likely to cause serious harm to the physical or mental health of the individual or someone else.
    2. Personal data that consists of educational records or relates to social work is also exempt from the subject access provisions where disclosure would be likely to prejudice the education or the social work of the individual.
    3. Decisions on the application of these exemptions are made by the relevant case worker with the Data Protection Officer. In some cases, a relevant health professional may need to be consulted.
    4. See Appendix 1 for further details on relevant legislation for these exemptions.

## Other Exemptions to Subject Access in DPA 2018

* + 1. Self Incrimination (Schedule 2 s20)
    2. Corporate Finance (Schedule 2 s.21)
    3. Management Forecasts (Schedule 2 s.22)
    4. Negotiations (Schedule 2 s.23)
    5. Confidential References (Schedule 2 s.24)
* This exempts references for education, training or employment provided to, or received from, another organisation in confidence from the right of subject access. This includes references provided for former staff members.
  + 1. Exam Scripts and Papers Schedule 2 s.25)
    2. Journalistic, academic, artistic and literary purposes (Schedule 2 s.26)
    3. Research and Statistics (Schedule 2 s.27)
    4. Archiving in the public interest (Schedule 2 s.28)
* The rights to access, rectification, erasure and portability do not apply where allowing these requests would prevent or seriously impair the achievement of those purposes.

# Procedure

* 1. Subject Access Requests, and other rights exercised by individuals, can be made most easily in writing (email, letter or online) to:

Email: [dp@cheshireeast.gov.uk](mailto:dp@cheshireeast.gov.uk)

Compliance & Customer Relations

Cheshire East Council

1st Floor, Westfields

c/o Municipal Buildings, Earle Street, Crewe CW1 2BJ

Website: <http://www.cheshireeast.gov.uk/council_and_democracy/council_information/data_protection/data_protection.aspx>

* 1. Requests could also be submitted via social media sites, e.g. Facebook, Twitter although it is not appropriate to respond via these methods.
  2. Verbal requests must still be actioned, although we may still need to verify the identity of the individual. Officers taking verbal requests who are unsure of what information is required can refer to the online form when eliciting information. If they fill in the online form themselves this will automatically pull through to the DP team, otherwise they should email through any details they take to [dp@cheshireeast.gov.uk](mailto:dp@cheshireeast.gov.uk) so that it can be logged.
  3. We need to be certain the request is coming form the correct individual. Where we are uncertain of the identity of a requester, two forms of identification are usually required to confirm the identity of the data subject, one which confirms their identity and one which confirms their current address. For example, one document from each list. Other documents may be considered in exceptional circumstances.

## Acceptable proof of identity:

* Current Passport
* Full birth certificate
* Unexpired photo card driving licence (full or provisional)

## Acceptable proof of current address:

* Utility bill dated within the last three months
* Bank statement dated within the last three months
* Benefits Agency/State Pension correspondence (on letterhead) dated within the last three months
* Council Tax bill for current year
* Unexpired old style paper driving licence
* Unexpired photo card driving licence (full or provisional)
  1. Photocopies, photographs or scans are acceptable provided they are clear and legible.
  2. In most cases no fee is chargeable.
  3. All requests will be logged by Compliance & Customer Relations. The team will validate the request and allocate to the relevant departmental co-ordinator(s) depending on the information being requested. The correct email address is [dp@cheshireeast.gov.uk](mailto:dp@cheshireeast.gov.uk).
  4. Departmental co-ordinators are responsible for collating all information held by their department and highlighting any information they believe should not be disclosed. Compliance & Customer Relations will send out the response.
  5. Requests must be responded to as soon as possible and, in any event, within one month of receipt of the request and any information required to locate the information held.
* This date is calculated as the corresponding date in the next month, starting with the day received e.g. request received 1st May – response is due 1st June
* If the next month does not contain a corresponding date then the last day of the month is used e.g. 30th January – 28th February
* If this date falls on a weekend or bank holiday then the next working day is used.
  1. If a request is particularly complex, or if multiple requests have been made by the same individual, we can apply up to a further 2 month extension to the time limit of the request. It is important to note that volume of data alone does not meet the definition of complexity set down by the GDPR/DPA 2018. The burden of proof rests with the Council to demonstrate the complexity of the request to warrant any extension of the time limit and advice from the Data Protection Officer should be sought before attempting to apply an extension. The individual must be informed of the application of any extension within one month of receipt of the request and any information required to locate the information held. The bullet points in 13.11 above also apply to the time periods mentioned here.
  2. Individuals can appoint an agent or representative to make a request on their behalf and that person’s identity will also need to be verified. Written authority from the individual giving permission for the representative to act for them is also required.
  3. In the case of active social services records, informal access to information should be a normal part of casework to ensure service users and carers are aware of the information held about them and the reasons it is held.
  4. Requests from post care adults who want access to their care files will be dealt with by the Access to Records Officer based within Compliance and Customer Relations. In the case of young care leavers, the Access to Records Officer will liaise with the relevant 16+ personal adviser to ensure the young person is considered mature enough to access their records and has adequate support during the process.

# Complaints/Appeals

* 1. If an individual is not satisfied with the response received as a result of their Subject Access Request, they may complain to the Compliance and Customer Relations Department in the first instance. If still not satisfied, individuals have a right of appeal to the Information Commissioner’s Office (ICO).
  2. The ICO will consider the nature of the complaint and make an assessment on whether the Council has complied with the legislation. This can result in regulatory action.

For further advice and guidance please contact the Data Protection Officer on 01270 686606, Assistant Data Protection Officer on 01270 685909, Access to Records Officer on 01270 686605 or email at [dp@cheshireeast.gov.uk](mailto:dp@cheshireeast.gov.uk)

# Appendix 1 – Legislation

In most cases the [GDPR](https://gdpr-info.eu/) or the [DPA 2018](http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) will give sufficient grounds for disclosing or withholding personal data but in the case of social services information in particular, other statutes should be considered.

### Art. 15 GDPR Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
   1. the purposes of the processing;
   2. the categories of personal data concerned;
   3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
   4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
   5. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
   6. the right to lodge a complaint with a supervisory authority;
   7. where the personal data are not collected from the data subject, any available information as to their source;
   8. the existence of automated decision-making, including profiling, referred to in[Article 22](https://gdpr-info.eu/art-22-gdpr/)(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to [Article 46](https://gdpr-info.eu/art-46-gdpr/) relating to the transfer.
3. 1The controller shall provide a copy of the personal data undergoing processing.2For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. 3Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

### Art. 17 GDPR Right to erasure (‘right to be forgotten’)

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
   1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
   2. the data subject withdraws consent on which the processing is based according to point (a) of [Article 6](https://gdpr-info.eu/art-6-gdpr/)(1), or point (a) of [Article 9](https://gdpr-info.eu/art-9-gdpr/)(2), and where there is no other legal ground for the processing;
   3. the data subject objects to the processing pursuant to [Article 21](https://gdpr-info.eu/art-21-gdpr/)(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to [Article 21](https://gdpr-info.eu/art-21-gdpr/)(2);
   4. the personal data have been unlawfully processed;
   5. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
   6. the personal data have been collected in relation to the offer of information society services referred to in [Article 8](https://gdpr-info.eu/art-8-gdpr/)(1).
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
   1. for exercising the right of freedom of expression and information;
   2. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   3. for reasons of public interest in the area of public health in accordance with points (h) and (i) of [Article 9](https://gdpr-info.eu/art-9-gdpr/)(2) as well as [Article 9](https://gdpr-info.eu/art-9-gdpr/)(3);
   4. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
   5. for the establishment, exercise or defence of legal claims.

### Art. 21 GDPR Right to object

1. 1The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of [Article 6(](https://gdpr-info.eu/art-6-gdpr/)1), including profiling based on those provisions. 2The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding [Directive 2002/58/EC](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058), the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to [Article 89(](https://gdpr-info.eu/art-89-gdpr/)1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

### Exemptions etc from the GDPR - Data Protection Act 2018 SCHEDULE 2

**PART 1**

**Adaptations and restrictions based on Articles 6(3) and 23(1)**

*GDPR provisions to be adapted or restricted: “the listed GDPR provisions”*

1 In this Part of this Schedule, “the listed GDPR provisions” means—

(a) the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the GDPR)—

(i) Article 13(1) to (3) (personal data collected from data subject: information to be provided);

(ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);

(iii) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);

(iv) Article 16 (right to rectification);

(v) Article 17(1) and (2) (right to erasure);

(vi) Article 18(1) (restriction of processing);

(vii) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(viii)Article 20(1) and (2) (right to data portability);

(ix) Article 21(1) (objections to processing);

(x) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (i) to (ix); and

(b) the following provisions of the GDPR (the application of which may be adapted by virtue of Article 6(3) of the GDPR)—

(i) Article 5(1)(a) (lawful, fair and transparent processing), other than the lawfulness requirements set out in Article 6;

(ii) Article 5(1)(b) (purpose limitation).

*Crime and taxation: general*

2 (1) The listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the following purposes—

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of a tax or duty or an imposition of a similar nature, to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

(2) Sub-paragraph (3) applies where—

(a) personal data is processed by a person (“Controller 1”) for any of the purposes mentioned in sub-paragraph (1)(a) to (c), and

(b) another person (“Controller 2”) obtains the data from Controller 1 for the purpose of discharging statutory functions and processes it for the purpose of discharging statutory functions.

(3) Controller 2 is exempt from the obligations in the following provisions of the GDPR—

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided),

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers), and

(d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a) to (c),

to the same extent that Controller 1 is exempt from those obligations by virtue of sub-paragraph (1).

The Statutory Instrument 2000 No 415 - The [Data Protection (Subject Access Modification) (Social Work) Order 2000](http://www.legislation.gov.uk/uksi/2000/415/contents/made) refers to personal data that, if disclosed, would prejudice the carrying out of social work by way of causing serious harm to the physical or mental health or condition of the data subject or any other person.  The professional opinion of a Social Services practitioner involved in the specific case will be relied upon for this judgement decision.

There is also a Statutory Instrument 2000 No 413 – [The Data Protection (Subject Access Modification) (Health) Order 2000](http://www.legislation.gov.uk/uksi/2000/413/contents/made) which specifically applies to information about the physical or mental health or condition of the data subject.  If disclosure would prejudice the carrying out of social work by way of causing serious harm to the physical or mental health or condition of the data subject or any other person, the opinion of an appropriate health professional should be sought.

# Appendix 2 - Other Guidance

The Information Commissioner’s Office provides a number of guidance documents on the right of subject access, the main ones being:

[Guide to GDPR](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/)

[Code of Practice for Dealing with Subject Access Requests](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/)