Isle of Man
Freedom of Information Act 2015

information commissioner
Barrantagh Fysseree

EXEMPTION NOTE

Section 25
Absolutely exempt personal information

This note is one of a series intended to provide practical guidance on the exemptions set out in the Isle of Man Freedom of Information Act 2015 (FOI).

Requests for information must be considered on a case by case basis and the Information Commissioner will review decisions on the facts of each case.

PO Box 69, Douglas, Isle of Man, IM99 1EQ T: +44 1624 693260 W: inforights.im E:ask@inforights.im

THE EXEMPTION

Section 25 states:

25 Absolutely exempt personal information

(1) Information is absolutely exempt information if it constitutes —

(a) personal data of which the applicant is the data subject;
(b) personal census information; or
(c) a deceased person's health record.

(2) Information is also absolutely exempt information if —

(a) it constitutes personal data of which the applicant is not the data subject; and
(b) one of the following applies —

(i) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the *Data Protection Act 2002*, the disclosure of the information to a member of the public (otherwise than under this Act) would contravene any of the data protection principles;

(ii) in a case where the information falls within paragraph (e) of that definition of "data", the disclosure of the information to a member of the public (otherwise than under this Act) would contravene any of the data protection principles if the exemptions in section 29A of the *Data Protection Act 2002* (manual data held by public authorities) were disregarded;

(iii) by virtue of a provision of Part 4 of that Act, the information would be exempt from section 5 of that Act (right of access to personal data) if the applicant were the data subject.

(3) Subject to subsection (4), words and phrases defined in the *Data Protection Act 2002* have the same meaning in this section as they have in that Act.

(4) In this section —

"census information" means any information —

(a) acquired by a person employed in taking a census under the *Census Act 1929* in the course of the person's employment; or
(b) derived from information covered by paragraph (a);

"health record" (including any related expression) has the meaning given by the *Access to Health Records and Reports Act 1993*; and

"personal census information" means census information that relates to an identifiable person or household.

THE MAIN POINTS

1. This is an absolute exemption which means the PA does not have to consider whether disclosure of the information would be in the public interest.

2. Section 25 provides a number of distinct exemptions which a PA may apply to a request for information concerning personal information.

Subsection 25(1)

3. The three exemptions set out in sub section 25(1) are intended to prevent information being disclosed under FOI when an applicant makes a request for :

    - personal data about themselves;
    - personal census information; or
    - a deceased person's health record.

Personal data of which the applicant is the data subject

4. The effect of this exemption is not to deny an applicant the right of access to information about themselves but to ensure that the request is made under the Data Protection Act 2002 (DPA) and that information (personal data) is provided in accordance with the DPA's provisions.

Personal census information

5. To apply this exemption the request must seek information acquired or derived by the PA under the Census Act 1929 which relate to an identifiable person or household.

6. Under the Census Act, individuals are required to make returns providing a variety of personal and sensitive personal data about themselves and family members in the household. In addition it is an offence for any person employed in taking a census to disclose any census information to another person.

7. This exemption is intended to ensure that a PA does not disclose census information in response to a request for information under FOI.

Deceased person's health record

8. Under the Access to Health Records and Reports Act 1993, only the personal representative of a deceased person can access their health record.

9. This exemption is intended to ensure that a PA does not disclose information from the health record of a deceased person in response to a request under FOI.

10. The exemption does not apply to other records of a deceased person, for example the exemption cannot be applied to any social work or educational record of a deceased person.

Subsection 25(2)

Disclosure of personal data to a third party

11. Subsection 25(2) sets out two distinct exemptions that a PA may apply when a request seeks information which is the personal data of another individual.

12. Subsections 25(2)(b)(i)&(ii) provides an exemption from the disclosure of third party personal data when disclosure would contravene any of the data protection principles. (see Other Considerations)

13. Subsection 25(2)(b)(iii) provides an exemption from disclosure when the third party personal data would not be disclosed to that third party under the DPA . That is if the data would not be disclosed to data subject exercising their right of access to personal data under the DPA then the PA must not disclose the data under FOI.

OTHER CONSIDERATIONS

1. The purpose of FOI as set out in section 3 is to make information available while maintaining amongst other things a balance with the rights to privacy. FOI does not override the right to privacy; on the contrary, the right to privacy has been upheld by Courts and Tribunals in the UK on several occasions.

2. To properly consider a request that seeks disclosure of information which includes a third party's personal data, the PA must have a good understanding of the DPA.

3. A PA must be mindful of all eight data protection principles. However in most cases the decision to withhold or disclose personal data to a third party is likely to be determined through consideration of the first and second data protection principles.

4. The first and second data protection principles require that "personal data are processed fairly and lawfully" and "personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose."

5. A PA should consider the generality of the second principle first. A disclosure under FOI is a disclosure to the world. The PA should consider whether a disclosure to the world of personal data it processes, for example via social media, would, in general terms, be compatible with the purpose for which the PA obtained the data.

6. There are three intertwined aspects to the first data protection principle which must all be met. Personal data must be processed:

   i. fairly,
   ii. lawfully, and
   iii. at least one condition set out in Schedule 2 to the DPA, and in the case of sensitive personal data a further condition set out in Schedule 3, must be met.

DPA Schedule 2 and 3 conditions

7. With regard to "sensitive personal data" the PA must consider whether the proposed disclosure to a third party (i.e. the applicant/world) would meet a lawful condition for processing set out in schedule 3 of the DPA. Unless the PA obtains the explicit consent of the data subject it is unlikely that a disclosure would comply with any other condition set out in schedule 3.

8. With regard to the disclosure of a non-sensitive personal data to a third party (i.e. the applicant/world), the only schedule 2 conditions that are likely to apply are consent of the data subject or the 'legitimate interests' condition.

9. The 'legitimate interests' condition states that the processing (in this case disclosure to the applicant/world) is "necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject."

10. The PA must consider:

i. What legitimate interests are being pursued by the applicant?
There is no definition within the DPA of the term "legitimate interest". When assessing whether an applicant has a legitimate interest, the PA could ask the applicant why they want the information (unless it is already clear from the information request or from previous correspondence.) PAs should remember, however, that applicants are not required to explain why they want the information if they do not wish to do so.

In some cases, the legitimate interest being pursued might be personal to the applicant – e.g. they might want the personal data in order to bring legal proceedings. With most requests, however, there are likely to be wider legitimate interests pursued, such as scrutiny of the actions of public bodies or public safety.

ii. Is the disclosure <u>necessary</u> for the legitimate interests identified?
A PA should consider whether it is necessary to disclose the third party personal data in full in order to pursue these legitimate interests or whether there are other methods which would still meet these interests without interfering with privacy.

iii. Would the disclosure of the data subject's personal data to a third party be unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject?
If the PA decides that the disclosure is necessary for the legitimate interests of the applicant, it must go on to consider whether the disclosure of the data would be unwarranted because it prejudices the data subject in some way. For example, disclosure of personal data to a third party will intrude into the data subject's privacy but it is not always unwarranted.

The rights and interests of the data subject must, therefore, be balanced with the identified legitimate interests of the applicant in receiving information and PAs must consider all of the circumstances in each case.

Factors to be taken into account include:

- Whether the information relates to the individual's public life (i.e. their work as a public official or employee) or their private life (i.e. their home, family, social life or finances).

- Information about an individual's private life will deserve more protection than information about an official or work capacity.

- The seniority of their position and the public facing role.
  The more senior a person is, the less likely it is that disclosing information about their public duties will be unwarranted or unfair.

- In general information about a senior official's public life should be disclosed unless it reveals details of the private lives of other people, such as their family.

- The potential harm or distress that may be caused.
  The PA should consider the harm or distress that the disclosure may cause the data subject in a personal as opposed to professional capacity. For example, what distress could be caused by the release of private information about family life? Other considerations could include whether disclosure of the information could harm the data subject, for example could disclosure of bank account details result in a risk of fraud, or could the disclosure cause risk to the data subject's health or personal safety? In such circumstances a disclosure is unlikely to be warranted.

- Whether the individual has objected to the disclosure.
  An objection is a factor to take into account, but it is not by itself sufficient to make the disclosure unwarranted or unfair.

- The reasonable expectations of the individual as to whether their information would be disclosed.
  In the absence of other factors disclosure will not be unwarranted or unfair just because the person was not aware of the possibility of disclosure.

Fairness

11. Any disclosure of personal data must be fair and the data subject should therefore be informed about this processing (disclosure) of their personal data. Factors to consider include:
    - Whether the individual expects their role to be subject to public scrutiny.
      Consideration should be given to the person's seniority, whether they have a public profile and whether their role requires a significant level of personal judgement and individual responsibility.
    - Whether any distress or damage would be caused to the data subject as a result of the disclosure;
    - Any express refusal by the data subject;
    - Whether the information relates to the data subject's public or private life. A person's private life is likely to deserve more protection.

Lawful

12. The PA should consider whether the disclosure would represent a breach of confidence or whether there is any statutory provision that prohibits disclosure.

13. If a PA is unable to identify a schedule 2 condition for processing (and schedule 3 in the case of sensitive personal data) then the disclosure would not be lawful.

14. A disclosure that contravenes any data protection principle would be unlawful.

DUTY TO ADVISE AND ASSIST

Section 15 requires PAs to provide reasonable and advice and assistance to persons who wish to make, or have made, requests for information.

If a public authority refuses a request on the basis that the information is accessible to the applicant under the Data Protection Act 2002 or the Access to Health Records and Reports Act 1993, then the PA must advise the applicant how and where to access that information and provide assistance, such as links to online information, to do so.

FURTHER RESOURCES

APPENDIX 1: IOM Commissioner Decisions & IOM Case law

APPENDIX 2: Other Commissioner Decisions & Case law

APPENDIX 1
IOM Commissioner Decisions & Case law

IOM Commissioner Decisions

Issue Date	Decision Number	Public Authority
26 August 2016	2016/0001	Cabinet Office
26 October 2016	2016/0003	Cabinet Office
4 August 2017	2017/0001	Chief Constable
12 December 2017	2014/0003	Department of Education and Children

IOM Case law

None

APPENDIX 2
Other Commissioner Decisions & Case law

Note
Neither the Commissioner nor the Court are obliged to follow decisions or case law from other jurisdictions.

UK Information Commissioner Decisions

www.ico.gov.uk/tools_and_resources/decision_notices.asp

Date	Reference	Public Authority
27 July 2016	FS50592465	Calderdale College
19 April 2016	FS50618570	London Borough of Islington
10 December 2014	FS50555821	Information Commissioner's Office

Scottish Information Commissioner (SIC) Decisions

The SIC's decisions are available at: www.itspublicknowledge.info/decisions

Decision Number	Parties	Summary
126/2009	Mrs Teresa Cleere-Martin and Glasgow City Council(GCC)	GCCl provided redacted versions of the minutes of the Young People's Sexual Health Steering Group, but withheld the names of individuals who were identified in the minutes and who had not consented to their names being disclosed. In relation to the lists of those attending the meetings in question and those submitting their apologies, the SIC did not agree that those names could be redacted. Whilst he agreed that the individuals could be identified from the information, it said nothing about them beyond their casual connection with particular meetings held on particular dates. It did not "relate to" the individuals in question and therefore was not their personal data. The SIC required this information to be disclosed. However, the SIC agreed that the GCC had been correct to withhold other information which was personal data. This information, which took the form of references to individuals in the text of the minutes, clearly associated these other individuals with specific aspects of work the Steering Group. The SIC accepted that these references focused on and were significantly biographical of those individuals and he accepted that the information related to them, and was personal data. As he was also satisfied that its disclosure would breach the first data protection principle, he accepted that the exemption applied
007/2011	Mr Gordon Aikman and the Chief Constable of Strathclyde Police	The SIC considered information concerning the security arrangements to be put in place when Abdelbaset Ali Mohmed Al-Megrahi left Greenock prison. Strathclyde Police considered that the information was all Mr Al-Megrahi's (or his family's) personal data, but the SIC disagreed. He noted that the focus of most of the information was the number of police officers to be involved, their roles, how long they would be working and how much the security arrangements might cost. Clearly, it could not be said that this type of information had no relevance at all to Mr Al-Megrahi or his family, but the focus of much of the information was not on Mr Al-Megrahi or his family and was not biographical in a significant way.

065/2005	Mr Camillo Fracassini of the Sunday Times and the Common Services Agency for the Scottish Health Service	The SIC concluded that, while details of the name and mortality rate of Scottish surgeons was indeed personal data, that data related to the professional lives of surgeons (as opposed to their private lives). The SIC went on to conclude that the release of the information would not breach any of the data protection principles, and required that it be released.
003/2007	Mr Allan McLeod and the Northern Joint Police Board	The SIC found, when considering a request for a summary report into Northern Constabulary's handling of complaints about an investigation into a death, that information comprising factual comments from witnesses made as part of their professional duties should, in the specific circumstances of that case, be released.
191/2007	Mr David Ewen of the Evening Express and Aberdeen City Council	The SIC found that the release of information relating to payments made to a number of former Council staff on their retirement (or redundancy) would be unfair, and the information should therefore not be released. In coming to this conclusion, the SIC took account of the fact that information concerning an individual's financial or contractual arrangement with their employer will relate to that individual's private life in a significant sense.
161/2007	Mr Michael McParlane and Strathclyde Fire Board	The SIC concluded that the release of the names and ranks of fire officers contained within a safety report would not be unfair, and ordered release. The officers in question were of senior rank, and held responsibility for fire safety and inspection. The SIC considered that persons holding the posts in question would have a reasonable expectation that their names would be available to members of the public, especially in relation to any professional duties in which they had taken part.
055/2007	Professor Ronald Macdonald and Highland Council	The case concerned a request for the qualifications of a particular employee. The SIC considered that the general level of the employee's post was not of sufficient seniority to ensure that the disclosure of personal data of this type would normally be expected. However, in this case, the SIC took the view that the specific nature and responsibilities of the post in question, which involved providing advice to the Council on matters of public safety gave rise to expectations of transparency and accountability. The SIC therefore concluded that the qualifications of the employee should be disclosed
033/2005	Paul Hutcheon, The Sunday Herald and the Scottish Parliamentary Corporate Body	The case concerned a request for the travel claims of David McLetchie MSP. On consideration of this issue, however, the SIC found, following a detailed review of the information, that no "pattern of movement" could be established, and that there would therefore be little, if any, risk of harm to Mr McLetchie as a result of release.

235/2006	Councillor William Buchanan and Falkirk Council	The SIC found that there was a genuine risk of harm should full details of the expense claims submitted by a named Councillor be released. In this case, a specific risk had been identified by the Council in relation to the Councillor in question, and the SIC was satisfied that the release of the information in question would expose the Councillor to that risk. The SIC accepted that, while such information would normally be released, the specific circumstances of this case ensured that disclosure would be unfair to the data subject.
003/2007	Mr Allan McLeod and the Northern Joint Police Board	The SIC found that the names of various officers mentioned in the complaint investigation report could be released. In coming to this decision, the SIC took into account the fact that the names were already publicly known, with some having been referenced in a publicly available Fatal Accident Inquiry report relating to the case.

Case law

UK Supreme Court

Date	Citation	Parties
29 July 2013	[2013] UKSC 55	South Lanarkshire Council v Scottish Information Commissioner

UK Tribunal decisions

Upper Tribunal

Date	Citation	Parties
22 June 2016	[2016] UKUT 0293 (AAC)	Illingworth v IC & NHS Commissioning Board
10 March 2016	[2016] UKUT 0139 (AAC)	Department of Health v IC & Bolton Council

First Tier Tribunal

Date	Citation	Parties
21 January 2016	EA/2016/0039	Roxburgh v IC & Mill View Primary School
10 June 2009	EA/2008/0084	Guardian News & Media Ltd v IC & Ministry of Justice