Information Rights: Freedom of Information and Data Protection Policy and Guidance

Team responsible for activity:	Policy
Activity normally carried out by:	*Policy and FOI Advisor*

Version:	4.0
Date version created:	March 2018

Written by:	Policy and FOI Advisor/ Data Protection Lead
Date last reviewed:	March 2018

Contents

Definitions and Abbreviations

Applicant	The person or organisation making a request and where the response is sent
Data Controller	A person who (either alone or jointly) determines the purposes and manner in which any personal data will be processed e.g. NHS Trust
Data Subject	An individual who is the subject of the personal data. They may also be the applicant, next of kin, or a member of staff making an internal request.
DPA, FOI(A), EIR	Abbreviations of laws, see Legal Framework below
ICO	Information Commissioner's Office
Personal data	Data referring to a living individual who can be identified from that data (or other information which is or likely to be in possession of the data controller). This includes any expression of opinion about the individual or indication of intentions of the data controller in respect of the individual. Examples include names, addresses, dates of birth and Hospital numbers.
SIRO	Senior Information Risk Owner
IAO	Information Asset Owner, provides support and evidence to requests
Staff	Anybody working on behalf of IPSA whether permanent employed, agency, bank, locum, contractor, volunteer or on work experience
D/SAR, request	Data/Subject Access Request - Application by or on behalf of the data subject under the Data Protection Act, for access to their information.

Legal Framework

- Data Protection Act 1998 (DPA) and Data Protection Act 2018 (enacted 23/5/18)
- Data Protection (Charges and Information) Regulations 2018 (c.f. Digital Economy Act 2017)
- General Data Protection Regulation
- e-Privacy (Privacy of Electronic Communications Regulation)
- Freedom of Information Act 2000 (FOI), Environmental Information Regulations 2004 (EIR)
  - Reuse of Public Sector Information Regulations 2015

Introduction

The Freedom of Information Act (2000) obligates IPSA:

- in respect of rights of access in relation to recorded information, subject to defined conditions and exemptions;
- to confirm whether information is held, and in cases where access to information is refused in reliance on an exemption from disclosure, to give reasons for that refusal;
- to provide reasonable advice and assistance to applicants approaching other public authorities who may have the information they seek;

- to adopt and maintain a publication scheme, which relates to operational transparency and public confidence, and to publish this information in accordance with the scheme.

The Data Protection Act obligates IPSA to:

- maintain safeguards ('Privacy by Design') that protects personal information;
- register with the ICO and pay prescribed charges;
- respond to SARs and other rights, where an individual writes asking for us to provide them with a copy of their personal information or to change the way IPSA processes their data;
- have legitimate documented reasons for collecting and using MPs personal data and to inform them on collection of the IPSA Privacy Notice and their rights;
- not use the data in ways that have unjustified adverse effects on MPs;
- handle MPs personal data only in ways they would reasonably and fairly expect; and
- ensure processing is transparent, fair, lawful, respecting the Principles of the Act and the rights of the subject, and that contracts and data sharing are also adequately designed.

All communications in writing to IPSA, including those transmitted by electronic means, may contain or amount to requests for information within the meaning of the Acts, and must be handled in accordance with the provisions of the Acts. Verbal communication does not constitute a request under the Freedom of Information or Data Protection Act. The full texts of the acts are available for reference on these websites:

Background

We have a duty to implement information rights as given in the legal framework listed earlier. The FOI legislation came into force on 1 January 2005, and provided members of the public with a right of access to information held by public authorities; to support openness and transparency across the public sector, and provide them with a greater understanding of how 'public' money is spent and how decisions are taken which affect the services provided to them.

Data protection laws give data subjects ("natural living persons") a suite of rights to confirm processing, the nature of that processing, and to potentially alter or halt processing.

This policy applies to all of our staff, whether permanent, temporary, locum or contractor staff. Others who may come into contact with personal data but are not actually employed by us, for example partner organisations and voluntary staff, have a contractual obligation to follow the requirements of confidentiality that any member of staff is expected to follow.

All information held is subject to the terms of the FOIA and DPA. This includes, but is not limited to:

- Correspondence – internal and external,
- Papers and minutes of meetings
- Recordings of phone calls
- Handwritten notes
- Financial data

- Policies and procedures
- Organisational charts
- Service information

Information marked 'confidential' or 'Official:Sensitive' will not necessarily be exempt from the legislation, and to be withheld will need to fall under one of the exemptions. Some exemptions may need the Qualified Person to form an opinion (FOI).

Responsibilities

IPSA recognises its responsibility under the Acts to provide a general right of access to our information. The **Chief Executive** has overall responsibility for Information Governance at IPSA.

The Senior Officer with overall responsibility for this policy is the **Director of Regulation.** They will manage Freedom of Information and Data Protection guidance, and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information.

The **Head of Policy and Assurance** is responsible for approving all responses to SARs and FOI requests.

The **Policy and FOI Advisor** will be the lead on all requests received by IPSA, facilitating the process from receipt through to drafting responses for approval by the Head of Policy.

The **Qualified Person** is a special role employed in Section 36 of the FOIA to offer their recorded 'reasonable opinion' that disclosure would prejudice effective conduct of public affairs. They will be a member of the Board with judicial experience. The ICO has detailed guidance for this FOI exemption.

The **Data Protection Officer** provides guidance and review of escalations of requests.

Information Asset Owners will support the discovery and interpretation of materials to be disclosed.

The **Publication Manager** is responsible for the extraction and redaction of images of receipts and invoices requested under the FOIA.

All managers are responsible for ensuring new members of staff receive an introductory briefing on the Freedom of Information and Data Protection Acts during their induction and that staff are aware of the statutory responsibilities of the organisation under the respective acts.

All staff are responsible for ensuring adherence to the terms of the FOIA and DPA, and for identifying requests made under those Acts and ensuring they are passed to the Policy and FOI Advisor.

IPSA's Publication Scheme

IPSA's Publication Scheme is available on our website at: www.theipsa.org.uk. The Publication Scheme specifies the information IPSA will make routinely available to the public as a matter of course and how it will do so.

IPSA is committed to making the following classes of information available to the public:

Who we are and what we do:

- Organisational information, contact details, constitutional and legal governance, details of senior staff members and how senior appointments are made.

What we spend and how we spend it:

- Financial information relating to projected or actual income and expenditure, tendering and procurement, publication of MPs' business costs and expenses, remuneration of senior staff and Board members, pay ranges for IPSA staff, information on how to make an FOI request

What our priorities are:

- Annual report, corporate plan and strategy

How we make decisions:

- Board minutes, public consultations and responses

Our policies and procedures:

- Scheme of MPs' Business Costs and Expenses and associated guidance, complaints procedure, records management policy, information assurance policy, gifts and hospitality code, staff expenses policy.

Lists and register

- Registers of interest, political activity monitoring form, conflicts of interests declarations, hospitality and gifts record, Board expenses

The services we offer:

- Letters sent to all MPs collectively, including any bulletins sent to MPs

Rights of access

The publication scheme noted above, approved following a public consultation including with the Information Commissioner, is referenced on our website.

However, members of the public can also make formal requests, regardless of whether they are acting in a personal or commercial capacity. We have a legal obligation under the FOIA and DPA to respond to these requests, and while these are coordinated by the Policy team, there is a responsibility on all staff to have knowledge of and comply with the Act, and respond promptly and accurately if they are assisting with requests. We should be helpful if they are not properly formed.

The FOIA and DPA establish two families of rights for the general public, with **no charge** for either:

- the right to be informed of processing and correcting(see later with other rights), and
- the right to receive the information (subject to exemptions).

Requests must:

- be in writing, which includes email messages;
- display the applicant's name and address (this includes an email address);
- highlight what information is required, or the rights(or actions) to address;
- if appropriate highlight the preferred method of delivery i.e. paper copy or electronic.

Applicants should direct requests to: FOI Officer (or DPO), IPSA, 4th Floor, 30 Millbank, SW1P 4DU, or to the allocated email address FOI@theipsa.org.uk and privacyrights@theipsa.org.uk

Should enquires or requests be received by IPSA (not having been sent to the proper address), they must be forwarded promptly to the FOI Team. At the discretion of the FOI Team some requests may be answered outside of the FOIA, as they can be considered 'business as usual' enquiries.

Request for personal data is exempted from the FOI process, and is handled under the DPA as a SAR.

Responding to Requests

Requests can be a handwritten note, received by post, email or similar (generally, they must be written, identify the requestor and adequately specify and describe the information sought.

IPSA keeps these mailboxes for requests: foi@theipsa.org.uk and privacyrights@theipsa.org.uk

If the request relates to information about the requestor (the person making the request) then this now becomes known as a **Subject Access Request** and is handled under the DPA. IPSA must be able to satisfy itself that the identity of the requestor is properly confirmed, or otherwise has the power to ask – such as a law firm, the Court service, a guardian or parent.

The request must give the name and a return email or postal address of the person requesting the information, and adequately describe the information that is being requested. IPSA is entitled to ask for more detail, if needed, to enable it to identify and locate the information sought.

Once a request is received from a department, it is the responsibility of the **Policy and FOI Advisor** to identify whether the information sought is held and if so to request it from the relevant team. That team should endeavor to provide the information within one week. The Policy and FOI Advisor will then draft a written response, to be approved by the Head of Policy and Assurance. Where the request has been made by the media, or may be of significant public interest, the Head of Communications should have prior sight of the response.

Not all information should be disclosed under the Freedom of Information Act or Data Protection Act. The following are typical examples of information which are exempt:

- Information which is prevented from being disclosed by law or exempt under the Freedom of Information or is otherwise considered to be protected from disclosure under the Data Protection Act. For example, MPs personal information including home address(es);

Further details on information which is exempt from disclosure under the FOIA can be found below.

Timeframes for response

IPSA must respond to any request made under the FOIA within **20 working days** although further reasonable details can be requested in order to identify and locate the information, or where consideration of the public interest test is required.

IPSA must respond to any SAR made under DPA within the **28 calendar days** (a month) after IPSA has clarified that the request is a SAR and satisfied itself as to the identity of the requestor.

Dealing with complaints

Stage one: internal review

If an applicant is unsatisfied with the way their request has been handled or the response they have received, they can ask for a review. IPSA has processes in place to ensure these are conducted in a timely manner, and following the timeframes specified within the legislation.

A copy of our internal review procedure for FOIA and DPA requests can be found on our website at: http://www.theipsa.org.uk/publications/freedom-of-information/

Stage two: complaining to the ICO

Should the applicant not be satisfied with the response from their internal review, they have the right to appeal to the ICO for a decision notice, who will investigate the procedures of responding to the request, and the answer provided, and they may make recommendations.

IPSA will support this process by cooperating fully with any requests for information from the ICO and responding to correspondence from the ICO within the timeframes they provide.

Records of requests and publication of responses

All FOIA and DPA requests received by IPSA and subsequent responses will be filed for future reference, in accordance with relevant retention timeframes.

Responses to all requests made under the FOIA will be published on our website at: http://www.theipsa.org.uk/publications/freedom-of-information/

Appendix A – Data Subject Access Rights (simplified for clarity)

This link explains the rights and expectations: https://gdpr-info.eu/chapter-3/

Right of access by the data subject

- to obtain 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(without infringing the rights of another) and the following information:
- the purposes of the processing; the categories of personal data concerned;
- 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; where the data was sourced
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- an explanation of their rights and complaints process
- the existence of automated decision-making, including profiling, and an explanation of what is involved
- the controller shall provide an easily consumable copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.

Right to rectification

- to obtain without undue delay the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed or corrected.

Right to erasure ('right to be forgotten')

- to obtain the erasure of personal data concerning them without undue delay where one of the following grounds applies:
- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground;
- the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- the personal data have been unlawfully processed;
- 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;

Right to restriction of processing

- the data subject shall have the right to obtain from the controller restriction of processing where:
- the accuracy of the personal data is contested by the data subject;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override their right
- where obtained, they shall be informed by the controller before the restriction is lifted.

Right to Notification regarding Rectification, Erasure, Restriction

- The controller will confirm actions taken to each third party recipient unless it involves disproportionate effort, and about those recipients if asked by the subject.

Right to Data Portability

- the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machinereadable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided where processing is based on consent and processing is by automated means.

Right to Object and Automated Decisions

- to object, at any time to processing of personal data concerning him or her which is based on processing by Public Sector bodies and organisations using legitimate interests as the processing basis, including profiling based on those provisions. The 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.
- where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing their data for such marketing, which includes profiling to the extent that it is related to direct marketing. That data shall no longer be processed for such purposes.

In recognising the above rights, any service designed should consider how that service can deliver against those rights. This will include discovery processes and tools, and Information Asset Owner support to help identify target records and record the Rights employed.

Appendix A2 – Data Subject "Playbook" – interpreting Rights

IPSA has an obligation to maintain lawful processing with other requirements placed upon it. It must maintain accurate records with proportional security, and only process information within those requirements and otherwise within its retention schedule. This means that when considering how to interpret and decide how best to respond to requests and rights, that none are treated as absolute rights, but instead considered within the context of what IPSA finds necessary to discharge its duties and obligations. In the event of clarity or dispute it is recommended that IPSA consider a response and lay out the position to explain what can and cannot be achieved. Any such response, along with the template letter should identify the Supervisory Authority (the ICO) and their complaints process.

IPSA must satisfy itself as to the identity of the requestor before responding, and confirm with what authority a third party is making the request: e.g. legal representation, Court Order, Guardianship.

Right of Access – the subject access rights should be completed as it always was, without prejudice to any third parties. The ICO has a Code of Practice which describes how to approach response. As above, an answer should lay out confirmation of types of data, purpose, any third parties, the retention periods and consider the application of other rights, such as rectification and erasure.

Right of Rectification – the subject has a right to ask for correction – to an accurate and demonstrably proven state – and not just to change to a desired entry. This rights assists IPSA with the principle of maintaining accurate records.

Right of Erasure ('forgotten') – the subject can reasonably expect that once necessary processing is completed that information is erased, and where otherwise discovered can use this right to confirm erasure. Excepting where there is a legal case (see Restriction), or within necessary retention periods, this right assists IPSA with record minimisation.

Right of Restriction – enables 3 capabilities which are to restrict processing of contested data until accuracy is established, to prevent the removal or erasure of data where there may be a legal case and normal practice would obstruct that case or discovery, or a legitimate interests test needs to be revisited (no such processing at the time of writing).

Right to Notification of Rectification, Erasure and Restriction – the subject may ask for confirmation that all third parties have been properly informed and who those parties are.

Right to Data Portability – at the time of writing, there is no other provider due to the regulatory nature and legal obligation on IPSA. This right should be explained that it cannot be applied.

Right to Object to Legitimate Interests processing and profiling – IPSA is not using legitimate interests or profiling at the time of writing.

Right to Prevent processing for Marketing – IPSA is not involved with marketing activities, which should be considered entirely separate from statutory consultation and operational newsletters.

The playbook is a guide and not absolute. Where there is no clear answer or the policy is incorrect though future clarity or precedent, further advice should be taken and the playbook updated.

Note the ICO advice below that some rights will not be available depending on the lawful basis.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawfulbasis-for-processing/

	Right to erasure	Right to portability	Right to object
Consent			✘ but right to withdraw consent
Contract			✘
Legal obligation	✘	✘	✘
Vital interests		✘	✘
Public task	✘	✘	
Legitimate interests		✘	

Appendix B - Exemptions under the FOIA

There are 23 exemptions under the Act, some exemptions where the public interest test applies, and others which are absolute exemptions.

A. Exemptions where the public interest test applies:

S22	Information intended for future publication
S24	National security
S26	Defence
S27	International relations
S28	Relations within the United Kingdom
S29	The economy
S30	Investigations and proceedings conducted by public authorities

S31	Law enforcement
S33	Audit functions
S35	Formulation of government policy, etc
S36	Prejudice to effective conduct of public affairs (except information held by the House of Commons or the House of Lords)
S37	Communications with Her Majesty, etc., and honours
S38	Health and safety
S39	Environmental information
S40	Personal information (Only where the information concerns a third party and a s.10 notice under the Data Protection Act 1998 applies to that information)
S42	Legal professional privilege
S43	Commercial interests

B. The absolute exemptions

If these exemptions apply it is not necessary to consider whether the disclosure is in the public interest.

S21	Information accessible to applicants by other means
S23	Information supplied by, or relating to, bodies dealing with security
S32	Court records, etc
S34	Parliamentary
S36	Prejudice to effective conduct of public affairs (only applies to information held by the House of Commons or the House of Lords)
S40	Personal information (where the applicant is the subject of the information)
S41	Information provided in confidence
S44	Prohibitions on disclosure where a disclosure is prohibited by an enactment or would constitute contempt of court

Appendix C - Decision Tree