

4. How to handle requests for data

It is in the very nature of a library and information service that it handles requests for information. Training in dealing with such requests should be a key component of staff training and development. Privacy issues are central to this process.

All UK organisations must operate within the confines of the Data Protection Act 1998. They will also be subject to other Acts that give the police and security agencies rights to demand access to personal data within specific contexts including the Police & Criminal Evidence Act 1984 and the Terrorism Act 2000. In general, where the disclosure of personal information is required by law or by order of a court, then it is exempted from the non-disclosure provisions within the Data Protection Act – such provision will cover areas such as child abuse. Public authorities listed in the Schedule to the Freedom of Information Act 2000 must also comply with that Act. This includes government departments, local and health authorities, maintained schools, FE institutions, universities and other HE institutions, as well as other listed public bodies including some museums. In Scotland the equivalent is the Freedom of Information (Scotland) Act 2002. Individual CILIP members need to have regard to the Ethical Principles (notably Principle three on access to information and Principle eight on respect for confidentiality and privacy of users).

It is important that the library and information service of any organisation is legally compliant. From time to time it may be necessary to take legal advice on this matter.



Checklist

The reflective practitioner should think about the following:

- How confident are you and other staff in dealing with requests for personal information about users (or other staff) from:
 - Members of the police or other regulatory or security officials?
 - Other departments within the organisation?
 - Members of the public?
 - External organisations?
 - Other?
- Does your organisation have a policy regarding the handling of such requests?
- Is any policy easily accessible? And properly publicised?
- Have staff been trained in the policy?
- Are you comfortable with the way individual cases have been handled by your organisation? If not, why not?

4.1 Requests from members of the public

It is important to establish whether the request for personal data relates to an individual's own personal data or that of somebody else. In the case of the former the request will constitute a 'subject access request' within the terms of the Data Protection Act 1998. In such cases it will be necessary for the individual to provide proof of identity and also to be clear whether they are interested only in the personal data held by the library and information service or want to know what the whole organisation has. Proper documentation of the procedure is essential.

When a person is asking for personal data about somebody else, then this will have to be looked at under the Freedom of Information Act 2000 (and its Scottish equivalent) where these Acts apply i.e. the public authorities and bodies outlined in section 4 above.

Other organisations will be under no legal obligation to consider supplying such data (and should not do so unless they can comply with the data protection principles restricting disclosure of personal data).

The term, 'third party data' is used to describe personal data about someone other than the applicant. In many cases, the request for information (under the Freedom of Information Act or otherwise) can and should be rejected, for example where disclosure of personal data would breach one of the data protection principles. One useful distinction is between 'public' personal data (public position held; expenses claimed etc) as opposed to private personal data (home address, marital status etc) with the latter usually being off limits. However a sense of proportion needs to be kept in terms of the risk to the individual (the person whose data is being revealed). Public libraries will have many instances of people wanting 'third party data' without posing a real threat – neighbours, for instance, borrowing for a vulnerable person unable to get to the library and wanting to know if 'they've read this one before'. Often the resolution may only be a phone call away to get the permission of the person concerned.

However, in cases of difficulty it should be possible to refer the request to a designated member of staff or specialist unit within the organisation.

Checklist

- Does any policy set out how to deal with requests for personal data from members of the public? When their request relates to their own personal data? When their request relates to the personal data of somebody else?
- Is there a designated member of staff or specialist unit to whom more difficult requests can be made?
- Is the process properly documented?

4.2 Requests from other departments or partner organisations

Larger organisations, such as local authorities or universities, will often have a number of departments and many organisations will work in partnership with other bodies. It is important to understand who, in such circumstances, has the right to access the personal data. It is also important to know who 'owns' the information and has responsibility for ensuring its accuracy, currency and security.

The starting point for determining these things will be the registered purpose or purposes for which the personal data is being collected as this will determine who will need access to this data. As with personal data used only within the library and information service different members of staff may need different levels of access in order to perform their tasks and this should be reflected in the permissions structure used within the system. It is also important that an individual (the 'data subject') is informed as to who does have access to their personal data.

Checklist

- Does any policy of your organisation set out how requests for personal data from other departments within your organisation or partner organisations should be dealt with?
- In cases of difficulty is there a designated member of staff or specialist unit to whom such requests can be passed?
- Are such requests for personal data properly documented to ensure an audit trail?
- Where data is shared between departments or partner organisations have proper arrangements been put in place to ensure that good practice is adhered to in the management and use of such personal data? (See also see section 2.3 on data sharing.)

4.3 Requests from the police and other security agencies

The police and other security agencies have powers to request or demand access to personal data under a number of different statutes. These include, for instance: the Data Protection Act 1998, Terrorism Act 2000, and Police and Criminal Evidence Act 1984. The Regulation of Investigatory Powers Act 2000 may also be relevant (see section 4.5). Each statute sets out a different authorisation procedure. Generally it is important to establish that the police are requesting personal data for a specific purpose (e.g. in regard to a specific arrestable offence) and are not simply on a 'fishing expedition'. In addition it is important to ensure that the proper authorisation procedure has been followed in each case.

Unless the police have invoked specific powers under one of the Acts there is no general obligation to answer police questions. However, if there are continuing concerns about responding to the police requests when such powers have been invoked, or responding to a court order or notice requiring disclosure of information, then urgent legal advice should be sought.

There are some instances when failure to report a matter to the police can be a criminal offence in itself. Under Section 38B of the Terrorism Act 2000, for instance, it is a criminal offence for a person to fail to disclose, without reasonable excuse, any information which they know or believe might help prevent another person carrying out an act of terrorism or might help in bringing a terrorist to justice in the UK. Where there is doubt about the legal obligations of individuals or an institution legal advice should be sought.

Checklist

- Does any policy of your organisation set out the procedure for dealing with requests for personal data from the police?
- Is there a designated member of staff or unit within the organisation to whom such requests should be referred?
- Are there proper request and authorisation forms to ensure an audit trail for such requests?
- What happens if a request is made outside 'office hours'?

4.4 Electoral registers

Library staff should be aware of the access restrictions to the full versions of current electoral registers. They can only be consulted under supervision and copied solely by means of hand-written notes. No form of photographic, mechanical or electronic copying is permitted by law. The law also prohibits a library from disclosing any information from full versions of the electoral registers over the phone or in writing or by allowing electronic copying for a period of ten years from the date of issue.

4.5 Covert interception of communications or surveillance

The Regulation of Investigatory Powers Act 2000 may also be relevant. This provides powers for the police and other authorities (including, for instance, local authorities) to mount covert surveillance or interception of communications with proper authorisation. Therefore it is about collecting new information rather than seeking access to existing information but it could involve the use of library systems, facilities or premises.

Further information

- Information Commissioner's Office (2009) [The Th!nk privacy toolkit](#)
- CILIP (2004) [Ethical Principles for library and information professionals](#)
- [Data Protection Act 1998](#)
- [Environmental Information Regulations 2004 \(full original text, not updated version\)](#)
- [Freedom of Information Act 2000](#)
- [Freedom of Information \(Scotland\) Act 2002](#)
- [Legal opinion of James Eadie, commissioned by CILIP 2005, on Police access to library user records](#)
- [Police & Criminal Evidence Act 1984](#)
- [Terrorism Act 2000](#)
- [Regulation of Investigatory Powers Act 2000](#)