



Data Protection Policy

Impetus keeps certain information about its members/clients, staff, Board Members and volunteers in order to run effectively and efficiently for the benefit of those we serve.

To comply with the law information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The following policy sets out how this will be achieved.

Definitions

Personal data is information about identifiable, living individuals held on computer or in most manual filing systems.

The Data Controller is Impetus under the Act and the Impetus Board Members are ultimately responsible for the policy's implementation.

The Policy

In keeping information about its members/clients, staff, Board Members and volunteers, Impetus will follow the eight Data Protection Principles set out in the Data Protection Act 1998, which are summarised below:

- Personal data must be obtained and processed **fairly** and **lawfully**
- Data can **only** be collected and used for **specified purposes**
- Data must be **adequate, relevant and not excessive**
- Data must be **accurate** and **up to date**
- Data must not be held any longer than necessary
- Data Subjects' rights must be respected
- Data must be kept safe from unauthorised access, accidental loss or damage
- Special rules apply to transfers abroad

Impetus staff, Board Members and volunteers who process or use any personal information in the course of their duties will ensure that these principles and the following procedures are followed at all times.

When Impetus has cause to obtain personal data (such as names, addresses, phone numbers, fax numbers, email addresses) from members/clients, this

data will be obtained, stored and processed solely to assist staff and volunteers in the efficient running of the service requested by the members/clients. Personal details supplied by members/clients will only be used to send them material that is considered potentially useful.

Personal data from new members/clients is collected over the phone and using other methods such as e-mail. During this initial contact, the member/client will be given an explanation of how their personal data will be used. Written consent will not be requested from members/clients as it is assumed that consent has been granted when a client freely gives their own details.

When a referral is made via a third party, contact may be made with the potential client to ensure that permission has been granted to store and process their personal data.

A member's/client's personal data will not be passed on to anyone outside Impetus without explicit consent from the member/client unless there is a legal duty of disclosure under other legislation, in which case Impetus' Chief Executive will be consulted. Contact details held on the Impetus database may be made available to groups/individuals outside of Impetus. Members/clients will be made aware of this when their details are being collected for the database and their verbal or written consent is requested.

Only Impetus staff and volunteers will normally have access to members'/clients' personal data. All staff and volunteers will be made aware of Impetus' Data Protection policy and their obligation not to disclose personal data to anyone who is not authorised to have it.

Members/clients will be supplied with a copy of any of their personal data held by Impetus if a request is made. It is currently Impetus's policy to supply this information free of charge.

Accuracy and Longevity

Impetus staff and volunteers will take reasonable steps to keep personal data up to date and accurate and make corrections in a timely fashion. Personal data will be stored for as long as the member/client uses our services and normally longer. Where a member/client ceases to use our services and it is not deemed appropriate to keep their records, their records will be destroyed. However, unless explicitly asked by a member/client to destroy their details, Impetus will normally continue to hold them on file for future reference.

If a request is received from an organisation to destroy their records, Impetus will remove their details from our database and request that all staff holding paper or electronic details for the organisation destroy them. This work will be carried out by the Data Protection Officer. It is the responsibility of all Impetus staff to inform the Data Protection Officer if such a request is received. This

procedure also applies if Impetus is informed that an organisation ceases to exist.

Storage

Personal data are kept in paper-based systems and on a password-protected computer system. Every effort will be made to ensure that paper-based data are stored in organised and secure systems.

Use of Photographs

Board Members, staff and volunteers will conform to the guidelines for the correct handling of photographic materials as laid down in Appendix 1 and will use the approval forms attached thereto.

Personal Data Relating to Staff, Volunteers and Board Members

Impetus obtains personal data (names, addresses, phone numbers, fax numbers, email addresses), application forms, references and in some cases other documents from staff, volunteers and Board Members. This data is stored and processed for the following purposes:

- assessing the suitability of an applicant for a specified role
- to keep track of availability and other necessary details with respect to volunteering opportunities
- to distribute relevant Impetus material (for example, information packs) by post

The contact details of Impetus staff, volunteers and Board Members will only be made available to other staff, volunteers and Board Members. Any other information supplied on application will be kept in a secure filing system and will not be accessed during the day-to-day running of Impetus.

Contact details of staff, volunteers and Board Members will not be passed on to anyone outside Impetus without their explicit consent.

Staff, volunteers and Board Members will be supplied with a copy of their personal data held by Impetus if a request is made. It is currently Impetus' policy to supply this information free of charge.

Impetus will take reasonable steps to keep personal data up to date and accurate and make corrections in a timely fashion. Personal data will be stored for as long as the staff/volunteers/Board Members are involved with Impetus and possibly longer where deemed appropriate. Where a member of staff/volunteer/the Board ceases to be involved with Impetus and it is not deemed appropriate to keep their records, their records will be destroyed. The Chief Executive has ultimate responsibility for destroying personnel files.

In relation to storage of information, the same procedures apply to staff, volunteers and Board Members as apply to members/clients above

In relation to use of photographs, the same procedures apply to staff, volunteers and Board Members as apply to members/clients above.

Data Protection Policy

Appendix 1

Guide to taking photos & using images of adults and children

Introduction

Since the introduction of the Data Protection Act in 1998, photographs and videos of clearly identifiable people are considered to be personal data. The following gives initial advice to Impetus staff and volunteers on taking and using images of adults and children in printed publications.

Data Protection Act 1998

You must get the permission of all people who will appear in a photograph or video image before you record the footage. That means children as well as adults.

Getting permission involves making it clear:

- Why you are using that person's image
- What you will be using it for, and
- Who might want to look at the pictures

Crowd Shots

If you are taking images at an event attended by large crowds, such as a festival, this is regarded as a public area so you do not need to get the permission of everyone in a crowd shot. People in the foreground are also considered to be in a public area. However, it is suggested that photographers address those within earshot, stating where the photograph may be published and giving them the opportunity to move away.

If you want to use an image of, for example, the winner of a prize – with the crowd in the background – you must get the winner's verbal permission and record the fact that you have done so. You can record their consent when you take the photograph or when you return to your office.

Planning

Before taking images of people, it is vital to get their consent. If the person is under 18 it is important to get consent from the parent, guardian or carer of any child or young person up to the age of 18.

A person's consent (or parental consent for those under 18) must be obtained when they are clearly recognisable in an image. A person may be unrecognisable if they have their back to the camera, or they appear out of

focus in the foreground of a photograph while the camera zooms in on an object in the background.

How long does consent last?

Images should be destroyed two years after the date on the consent form, unless further consent is agreed. This is particularly important if your publication will have a high profile, e.g. if it will have a wide circulation. If the images are for a specific project, you may want to state this on the form and agree not to use the photographs for other projects.

Using existing photographs

If you are re-using photographs featuring adults and particularly children who are clearly identifiable, check that consents are in place. If the consent only allowed for paper publications, ensure the consent is renewed if you intend to use the images in another medium.

If the photos are old the following criteria should be used:

- For what purpose was the photograph originally taken, e.g. was it taken for a specific project?
- Where was the photograph taken, e.g. was it taken in a public place?
- When was it taken, e.g. is it a picture of a child who could now be an adult?

Photographs should be destroyed once the consent has expired unless the consent is renewed.

Putting photographs on the web

You must ensure that you have consent to do so as this will be available worldwide and you do not have control over who looks at this or how the image may be re-used. You must be particularly sensitive in the use of images of children.

Using photos of staff on the Internet or intranet

Consent from staff members should be sought before photographs are used in printed or website publicity.

Using photographs from a designer or an agency

You should ask the designer or the agency to guarantee that permission has been granted. You should also tell the designer or the agency how you will be using the photographs because this could affect the permissions. Ultimately, however, it is your responsibility to ensure that the designer or the agency got permission from the people in the photographs, so you might want to get this in writing from the agency.

Getting consent

To avoid any problems in the future, you must always get a signed consent form before taking any images. For children, you need the consent of the parents.

What else should I think about?

You will also need to be aware of **copyright implications** with any photographs that you may use from elsewhere.

Videos

Before any adults or young people up to the age of 18 can appear in a video, you must get the correct permission, i.e. parental consent for those under 18. You can do this in the same way as for photographs of people, using the relevant consent form. Similarly, you must get the permission of anyone in your video that is not part of a crowd and is easily recognisable.

Data Protection Policy

Appendix 2

Guidelines for Staff Members, Volunteers and Board Members

During the course of your duties with Impetus, you will be dealing with information such as names/addresses/phone numbers/e-mail addresses of members/clients/volunteers. You may be told or overhear sensitive information while working for Impetus. The Data Protection Act (1988) gives specific guidance on how this information should be dealt with by organisations such as Impetus. In short, to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To help you meet the terms of the Data Protection Act while working for Impetus, the following guidelines have been drawn up. Please read them carefully and ask the Data Protection Officer or Chief Executive if you are in any doubt about any of them.

Sharing members'/clients' personal information

"Personal information" includes details such as addresses/phone numbers and health details supplied by members/clients. Such information may be shared between staff and volunteers at Impetus for work reasons, but should not be given to anyone outside Impetus without explicit consent from the member/client. If such a situation arises, please ask a fellow member of staff for advice.

New members/clients

All requests from new members/clients for any service offered by Impetus should be referred to the appropriate member of staff. If the appropriate member of staff is not available, please take a name and contact number only and pass the message on. This is particularly important when dealing with a third party (for example, if a relative or friend phones on behalf of someone else) as Impetus should not collect information about a person who has not given permission to use his/her details. In most cases however, it is assumed that if a representative of a group contacts Impetus then that group has given Impetus permission to use their details.

Unlawful disclosure of personal information

Under the Data Protection Act you are committing a criminal offence if you disclose personal information 'knowingly or recklessly' to anyone you are not supposed to, so please be careful. As Impetus has an open door policy for members of the public to drop in anytime during opening hours, please seek to ensure that conversations are as private as possible, and be aware that conversations containing personal or sensitive information may be overheard by people who should not have access to such information.

Use of files, books and other paper records

In order to prevent unauthorised access and accidental loss or damage to personal information held on paper, please take good care of the files, books and other paper records you use while on duty, and ensure that they are stored safely before you leave the building.

Disposal of scrap paper

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please tear up or shred such notes before disposing of them in the waste paper bin.