Data Protection Policy

1 Introduction

International Community Organisation of Sunderland (ICOS) is required by law to comply with the Data Protection Act, 2018 (DPA 2018) and the General Data Protection Regulation (GDPR). This Act came into force on 25th of May 2018 and relates to the holding and processing of personal information relating to individuals.
ICOS needs to keep certain personal information about individuals such as employees, members and others, defined as *Data Subjects* in the Act, to fulfil its objectives and meet legal obligations.
To comply with the law all data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Organisation must abide the data protection principles.

2 Data protection principles

ICOS is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Data should not be transferred to a country or territory outside the European Economic Area, unless that territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

This policy shall guide all who process data in the Organisation to ensure that these principles are followed and any breach, whether deliberate or through negligence, may lead to disciplinary action being taken.

2 Definitions

Processing is given a broad interpretation in the Act: it covers collecting, holding, sorting, destroying of data etc. Every person who holds any personal data about another individual in some form or medium (hard-copy or electronic) from where it can be retrieved is 'processing' data.
Personal Data is defined in the Act as data that relate to a living individual who can be identified from those data; or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller; and includes any expression of opinion about the individual and any indications of the intentions of the Data Controller or any other person in respect of the individual. Examples are name, address, date of birth, attendance details, comments on coursework, a photo.

1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
   This special category of sensitive personal data is information that relates to:

   His/ hers race or ethnic origin;
   political opinions;
   religious or philosophical beliefs;
   trade union membership;
   physical or mental health;
   an individual's sex life or sexual orientation;
   Genetic or biometric data for the purpose of uniquely identifying a natural person.

Note 1: personal demographic data are also considered to be sensitive (e.g. home address, salary, and bank financial details).
Note 2: This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Data Controller is the person or entity who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.[1] ICOS, as a corporate body, is the Data Controller under the Act; so are its employees and volunteers.
Data Processor is any person other than an employee of the Data Controller who processes data on behalf of the Data Controller. For example, this could be a supplier to which some service, such as a payroll, has been outsourced.
Data Subject is the living individual to whom the data relates. For example, for the Organisation this would mean employees and students, among others.

3 Rights to Access Information

The Act gives Data Subjects a right of access to personal data held about them by the Organisation, and allows the Organisation to charge a fee for such access.

All such requests to ICOS must be made in writing and a record must be kept of all requests for access to personal data. Access does not include the right to amend data, but the Data Subject has the right to request any errors or omissions identified are corrected.
All formal Subject Access Requests must be responded to within the terms laid down by the Act, and must be notified to the secretary as soon as they are received.
ICOS will ordinarily charge the prescribed maximum fee (currently £10) for Subject Access Requests and take steps to verify the identity of the applicant.

4 Responsibilities of the Data Controller and Data Processors

Compliance with the GDPR it is mandatory and disciplinary action may be taken against anyone who fails to do so. The accompanying Guidelines should also be followed.

Consent - In order to process data the Organisation shall obtain consent from Data Subjects. In the case of sensitive personal data, express consent must be obtained. Consent for processing data may be obtained in different ways including:

a. Face-to-face
b. E-mail
c. Telephone
d. Written

Consent must be recorded and maintained with the case records.

Data Security - All ICOS users of personal data must ensure that all such data they hold is kept securely, for example in a locked cabinet or password protected. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise. ICOS security measures will include:

a. ICOS shall ensure that all personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

Third Parties – If ICOS enters in to agreements with third parties which include the sharing of personal data it shall ensure that adequate protection is offered and will use the data in accordance with defined purposes

5 Responsibilities of Data Subjects

All Data Subjects have an obligation to:

Ensure that any information that they provide is accurate and up to date

Inform the College and/or their department of any changes to information which they have provided, e.g. changes of address

Inform the Organisation of any known errors

6 Retention of Data

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. This applies to both electronic and non-electronic personal data. The Organisation will keep some forms of information for longer than others.

7 Related Policies

IT Policy

8 Checklist for Processing Data

Anyone in the Organisation processing personal data shall consider the following

Is this information really needed?

Is the information 'standard' or 'sensitive'?

If it is *sensitive*, has the Data Subject's express consent been obtained?

Has the Data Subject been informed that this type of data will be processed?

Are you authorised to collect/store/process the data?

If yes, have you checked with the Data Subject that the data is accurate?

Will the data be securely held?

If you do not have the Data Subject's consent to process, are you satisfied that it is in his/her best interests to collect and retain the data?

How long does the data need to be kept and are there arrangements for its review/secure disposal?

9 General provisions

a. This policy applies to all personal data processed by the organisation.
b. The Responsible Person shall take responsibility for the organisations ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.

10 ICOS Duties

As required by the Act, the Organisation has notified the U.K. Information Commissioner that it processes personal data. Further information: office@icos.org.uk

Appendix – Guidelines

These Guidelines should be read in conjunction with the Organisation's Data Protection Policy. Examples are set out below to illustrate some of the scenarios staff in ICOS might experience and best practice to be adopted.

I. What are my responsibilities?

All staff will process personal data in one form or another and as such have a duty to ensure that this is done fairly, stored securely and disposed of when it is no longer required. As such, all staff should be aware of the GDPR principles and bear in mind the 'Checklist for Processing Data' detailed in the Policy. In particular, be aware of what constitutes sensitive personal data and the special circumstances under which it can be processed.

II. Dealing with Subject Access Requests

Anyone who wishes to make a Subject Access Request (SAR) should fill in an SAR Form available on the website. Data Controller, must respond to such a request, in full, within forty calendar days. There are certain requirements that must be satisfied by the Data Subject before the forty day period begins:

the request must be in writing, preferably using the appropriate SAR form

any fee must have been paid (not exceeding £10) †

the person making the request must have properly identified him/herself

enough information must be provided to locate the data (i.e. the request must be sufficiently clear as to what is being sought: a Data Subject can't simply say "give me everything you have on me" and expect a full response) *

there must not have been repeated or similar requests from the Data Subject unreasonably close in time (if so, it may not be necessary to respond)

there must not be a 'disproportionate effort' involved in responding to the request (although this is a difficult point to argue)

* data which may be produced in the event of an SAR is usually to be found in what the Act defines as a 'relevant filing system'. However, if the request contains a description of the data, the individual would have a right of access to unstructured data. For further details, please use the contact details below.

III. Processing data

When processing personal data it is important that this complies with the GDPR Principles. For example, at the point of collection the form or web page should state the purpose for collection and no data other than that required for that particular transaction should be collected. For help drafting such a fair processing notice please use the contact details below. It is good practice to keep a record of the consent given as an audit trail. The fair processing notice to students, displayed on (re-)enrolment, makes data sharing between departments possible. Also, appropriate security measures must be taken when storing, moving or transmitting data, such as encryption.

- What to do

At the point of collection the following information should be provided:

The identity of the Data Controller

The purpose(s) for which the data is being collected

The recipients to whom the data may be disclosed (or transferred)

Details of how to opt-out of any subsequent re-use

III (i) Storage and handling of data

Personal data should be marked with an appropriate classification as per SOP DG09 – Information Classification and stored and handled (and disposed of) as determined by these. Data is to be given appropriate levels of access control and security. This means that it should be safeguarded by means of lockable cabinets and password and/or encryption protection, depending on format. See SOP DG14 – Storage of Information and SOP DG15 – Handling of Information.
Handling and exchange of patient information must in addition comply with the Access to Health Records Act 1990 where only those with a professional or contractual duty of confidentiality are permitted access to patient information. Please also see the Records Management Procedures.
- What to do
Make sure you use passwords which are strong and hard to guess. Never share or write passwords down and keep a log of who has access to secure areas. Secure personal information physically by restricting access to only those who need it for the performance of their duties and lock cabinets, rooms and computers when the information is not in use.

III (ii) Sensitive data

Sensitive personal data should only be recorded when the Data Subject has given express consent. The only exceptions are when it is required in order to protect the vital interests of the individual or another person or in the administration of justice. See also the Advice and Counselling Service's Confidentiality and Data Protection Policy.
- What to do
When recording data like absences, extenuating circumstances or disciplinary offences on a file, only brief notes should be made with little or no detail e.g. "absent due to ill health".

IV. References

Internal references provided for the purposes of education, training or employment are exempt from SARs

External references sent to ICOS *may* only be released if consent has been given by the referee or if it is reasonable in all the circumstances

- What to do
Requests for references could routinely include a note asking the referee to indicate (non-) willingness for its release on request *or* if there is no consent, the text could be redacted so as to remove anything that would reveal the identity of the referee – in reality impractical. For example, Admissions' reference request form states, "Referees are asked to note that the applicant may seek disclosure of this reference under the provisions of the Data Protection Act".

References provided by ICOS are exempt from SARs made to it, but the Data Subject may see the reference if they make an SAR to the third party to whom the reference has been provided

In writing a reference the author should always indicate how long (s)he has known the individual and in what capacity. Again, comments must be factually accurate and honest and subjective personal opinions must be avoided. As a general rule, you are advised not to include information in a reference that you would not wish the individual concerned to see. Spent disciplinary sanctions must not be referred to (usually six years after case closure).

V. HR records

V (i) Disciplinary procedures

The outcome of grievances is only disclosable to the person who is the subject of the process, not to any other parties

- What to do

If there is a disciplinary process against an employee, then only that employee has a right to know the details of that process. For example if an accusation is made by a volunteer, member, client or member of staff against another member of staff, expectations should be managed from the start. The accuser does not have a right to be kept informed or to know the outcome of the process. Only tell them that the procedure has been completed when it has, but not how.

V (ii) Sick notes

Sick notes contain sensitive personal data and should only be seen by those who need to know

- What to do

Sick notes should not have to be seen by line managers unless explicit consent has been given by the employee.

VI. Images

Photos/video taken for official use are covered by the Act and people in them should be advised why they are being taken

Photos/video showing a crowd scene (e.g. in a public place) would not be considered to be personal data because the purpose of capturing the individuals is not to identify them

Photos of staff on the intranet need no consent but consent is required if the site is an Internet one

- What to do

Consent should be sought wherever possible, especially of individual shots because they can be readily identified. Where this is not practical for each individual, for example at an event or at a degree ceremony, Data Subjects should be made aware: a statement should appear on tickets/programmes and/or a notice be displayed explaining that photographs/video are being taken and the purpose to which these may be put. All photographers should be clearly identified, e.g. with a visible badge. If taking photographs of children consent must be obtained from a parent or guardian.

If a student or member of staff objects to having a photograph published, on a departmental website for instance, then it must be removed. Prior consent should be sought wherever possible.

I

VII. Direct marketing

Data Subjects have the right to ask organisations to stop, or not to start, direct marketing aimed at them

- What to do

It is accepted that, for example, a member may receive communication from ICOS> He/she will have, however an clear option of opting out from receiving these communications.

IX. Third parties/countries and outside agencies

The policy makes it clear that it is a serious offence to disclose any personal data to a non-authorised person, including orally. It can usually only be released with the Data Subject's consent, unless one of the exemptions is met or a court order issued.

When dealing with a third party acting as a Data Processor

When personal data may be transferred outside the EEA under adequate level of protection

- What to do

Personal data may be passed to partnering organisations in countries outside the EEA, such as BUPT, which do not have the same levels of protection for personal data as long as certain safeguards are in place (though there are some exemptions). In this case the other party may become a data processor. The ICO and the Data Subject must be informed prior to any transfer. Details of these safeguards and of standard contractual clauses which may be employed are available from the Records & Information Compliance Manager. See also section XI. below.

Individual enquiries e.g. from friends or relatives in person, by telephone, email etc. need to be handled with care

- What to do

The agency must complete a Section 29 form (available on request) to apply for access specifying the purposes for which it is required. The data must be necessary, not just helpful to these purposes. Even then Queen Mary is not compelled to release the data without the Data Subject's consent: rights and interests should be balanced in coming to a decision. NB Such an enquiry *may* also come from an investigation in to tax/benefit fraud or immigration e.g. from local government or the Home Office/Border Agency. It's important to verify the identity of anyone making such requests and ensure the request is counter-signed by an authorised individual. This should be someone who is senior in rank/position to the requester.

Protecting the vital interests of the Data Subject or preventing serious harm to a third party

- What to do

The consent of the Data Subject is not required if a failure to release data would result in her or a third party's harm or if required to perform a regulatory function, such as securing health and safety at work.

X. Which countries outside the European Economic Area have adequate protection for personal data?

The European Commission has recognised the following territories as having adequate data protection:

Argentina

Canada

Switzerland

Guernsey

Isle of Man

Jersey

United States (under safe harbor rules only)

XI. What other exemptions are there to the release of information?

Data protection legislation does not cover the deceased

Data may be released to the police or other law enforcement organisation in pursuit of an active investigation (see X. above)

Disclosure of data may be necessary in the case of a medical emergency

In addition, the Guidelines on the right to privacy and the monitoring of data give information on the rights of employees and the right of the Organisation to monitor employees' activities. Students should refer to the Fair Processing Notice that they view on (re-)enrolment too.

XII. What are the penalties for Data Controllers if they breach the law?

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, ICOS shall promptly assess the risk to people's rights and freedoms and report this breach.

Criminal prosecutions may be brought against not just the directors or trustees of an organisation but also other officers (i.e. employees) who are responsible for a breach. This personal liability is important to note

A Data Subject can bring a claim for compensation for a breach which resulted in their suffering damage or distress

A Data Subject can also apply to the courts for an order which: requires the Data Controller to comply with an SAR; requires it to stop processing their data where it is being used for direct marketing or is likely to cause damage or distress; or, requires erasure/rectification of data where it is inaccurate

The Information Commissioner may serve an enforcement notice on a Data Controller if an investigation results in a finding that one of the eight principles has been breached. The Information Commissioner sets out the remedial steps which need to be taken by the Data Controller in question and failure to comply with these instructions would also be a serious offence under the Act

Other legislation may be applicable, for example monetary penalties for data breaches can be issued under the Criminal Justice and Immigration Act 2008

XIII. Who has the authority to report any breaches?

Any (suspected) breaches should be notified to the U.K. Information Commissioner. Although there is no legal obligation on Data Controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his Office.