Office of the Scottish Charity Regulator

Data Protection Policy

Contents

Introduction..... 3

Who does this policy apply to?..... 3

Requirements of Legislation..... 3

Management and Responsibilities..... 4

The Data Protection Principles..... 4

Conditions for Processing..... 4

Privacy Notices..... 5

Disclosure of Personal Information..... 5

Necessary, relevant and accurate..... 6

Appropriate Language..... 7

Security: general..... 7

Security: communications..... 8

Processors..... 8

Reporting of incidents..... 8

The rights of individuals..... 9

Transfers of data outside of the United Kingdom..... 10

New processing activities..... 10

Staff Awareness..... 11

Introduction

The Scottish Charity Regulator (**OSCR**) is committed to protecting personal information in line with our obligations under data protection law.

This policy sets OSCR's obligations when processing the personal information of others in the course of our work.

Compliance with this policy will help OSCR to meet its objectives of:

- protecting individuals whose personal information we process
- maintaining confidence in our organisation and our reputation
- complying with our legal obligations – if our organisation fails to comply with data protection law, this can lead to significant sanctions, including substantial fines.

Who does this policy apply to?

This policy applies to all employees, contractors and volunteers that may process the personal information of others in their work for OSCR (together referred to as '**staff'** in this policy).

OSCR may amend this policy at any time. It will be reviewed annually, or as appropriate to take into account changes to legislation that may occur, and/or guidance from the Government and/or the Information Commissioner's Office (**ICO**).

Requirements of legislation

This policy sets out how OSCR meets its legal obligations and requirements under the Data Protection Act 2018 and UK GDPR (the **data protection legislation**). The data protection legislation establishes a framework of rights and duties which are designed to safeguard personal information. This framework balances the legitimate functions and other business needs of OSCR as an organisation to collect and use personal information against the rights of individuals to respect the privacy of their personal details.

In this policy, **personal information** means information about a living individual from which they can be identified (or from which they can be identified along with other information we hold or can reasonably access).

The data protection legislation imposes obligations on the use of all personal information held and processed by OSCR as a **controller**, whether it relates to charity trustees, charity beneficiaries, employees, complainants, contractors or any other individual who comes into contact with the OSCR. This has implications for every part of OSCR. **Processing** includes collecting personal information, recording

it, storing it, using it, amending it, destroying it and, in some circumstances, disclosing it.

Management and responsibilities

The Chief Executive, as Accountable Officer (**AO**), has overall responsibility for data protection within OSCR. The Head of Corporate is designated as OSCR's Senior Information Risk Owner (**SIRO**). The implementation of, and compliance with, this policy is delegated to the Data Protection Officer (**DPO**). The DPO for OSCR is the Team Leader: Office and Records Management.

All managers are responsible for ensuring that this policy is communicated and implemented within their area of responsibility. They are responsible for the quality, security and management of personal information in use in their area. Advice and guidance regarding this policy or the data protection legislation in general is available here or from the DPO.

The Data Protection Principles

The data protection legislation is underpinned by 7 principles.

Principle 1 – processing of personal data shall be lawful, fair and transparent
Principle 2 – personal data shall be collected only for one or more specified, explicit and legitimate purposes, and shall not be processed in any manner incompatible with the purpose(s) for which it is collected: - **a) unless the controller is authorised by law to process the data for that purpose, and** **b) the processing is necessary and proportionate to that other purpose**
Principle 3 – personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
Principle 4 – personal data undergoing processing must be accurate and, where necessary, kept up to date
Principle 5 – personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes for which it is processed
Principle 6 – personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data
Principle 7 – the controller must be able to demonstrate compliance with these principles

Conditions for processing

Before OSCR can process any individual's personal information we must ensure that the "conditions for processing" are met. The conditions for processing are stated in Articles 6 and 9 of UK GDPR. Further conditions for processing are applied when **special category personal data** is involved, such as information about an individual's health, religious or philosophical beliefs, sexual orientation, political

opinions, racial or ethnic origin, trade union membership, genetic data, biometric data used for the purposes of identification, or criminal convictions and offences.

Privacy notices

When personal information is collected about individuals, they should be told exactly how that information is to be used. This is called a "**privacy notice**" and it should tell them:

- our identity (business area)
- the reasons (purpose(s)) we intend to process the information; and
- anything extra we need to tell individuals in the circumstances to enable us to process the information fairly.

If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether or not to enter into the relationship.

In the course of its work OSCR must only process personal information in accordance with the published Privacy Notices.

All staff must ensure that they have read and understood the privacy notices and any relevant policies, guidelines and procedures. Staff should contact the DPO if they are unsure about any aspect.

The DPO must be contacted immediately if there any doubt as to whether any particular processing of personal information falls out with the terms of the relevant privacy notice or whether OSCR has a lawful basis for processing particular personal information.

Disclosures of personal information

Information about identifiable individuals should only be disclosed on a need to know basis (for example, in order to provide services to us).

Before sharing personal information, we must:

- comply with any policies, guidelines or procedures relating to the sharing of personal information
- only share personal information with another of our staff, or with one of our agents or representatives, if that person has a work-related need to know the information
- only share personal information with third parties (including, for example, our service providers) if:
    - they have a need to know the personal information (for example, in order to provide services to OSCR)
    - the relevant privacy notice gives notice that the personal information may be shared with that third party; and

- we are satisfied that the third party will comply with the data protection principles, in particular that the personal information will be kept secure.

Disclosures of information may occur because of a legal requirement such as with a Court Order. Specific legislation covers some disclosure (for example, for tax and pension purposes). The validity of all requests for disclosure of personal information without consent from the individual must be checked. The identity of those requesting data and their legal right to request or demand information must be validated. The reasons for disclosures made without consent must be documented.

Police officers or others requesting information for the purposes of a criminal investigation, including for benefit, tax or immigration offences, should be asked to put their request in writing, either by using a standard data protection request form, or by letter / email. This requirement can be set aside where the request is made in an emergency (i.e. a person is in immediate and imminent risk of serious harm).

The request should include:

- what information is needed
- why it is needed
- how the investigation will be prejudiced without it

Necessary, relevant and accurate

Personal information must not be re-used for any purpose that is incompatible with the original purpose for which it was collected.

Managers should ensure that any data collected from individuals is complete but not excessive, and the level of data retained on OSCR systems should be appropriate for current, existing purposes.

Staff should only access and process personal information that is necessary to perform their work. Staff must not access or process personal information for any reason unrelated to their work.

Information Asset Owners (**IAOs**) and team managers must ensure that personal information they are responsible for and stored in any way on any media is accurate and kept up to date.

The accuracy of staff information should also be checked on a regular basis – either by line managers or by HR.

Personal information must not be retained indefinitely, and managers must ensure that they are aware of, and compliant with, OSCR's Information Management policy and principles including the agreed retention schedules for all documents and files.

If staff are responsible for the deletion or anonymisation of personal information, this is done in accordance with any relevant privacy notice or policy. OSCR must not keep personal information for longer than necessary.

Appropriate language

Appropriate language must always be used if recording an opinion about an individual (for example, in an email or chat message).

OSCR must not mislead anyone as to how their personal information may be used.

Security: general

All information relating to identifiable individuals must be kept secure at all times. Managers must take steps to ensure that office environments and working practices take account of the security necessary to prevent the loss, theft, damage or unauthorised access to personal information. IAOs are responsible for ensuring that all systems storing personal information, or other assets or repositories of information are appropriately risk-assessed and protected from identifiable threats.

Personal information must be kept secure and OSCR's work performed in such a way as to protect the personal information that we hold. In particular, all policies must be complied with, guidelines and procedures that are put in place to secure personal information (including the use of any technology). Particular care must be taken in protecting special categories of personal information from loss or unauthorised access, use or disclosure.

No attempts to circumvent the safeguards OSCR uses to protect personal information (including administrative, physical and technical safeguards) are to be made.

All personal information must be stored in our IT systems.

Any paperwork containing personal information must be disposed of in the confidential waste bins provided on our premises. Do not create unnecessary copies of personal information.

Further advice on securing information can be found in the **IT Code of Conduct** and the **Information Security Summary**.

Security: communications

Staff should check that the addresses are correct on letters, emails or other communications that contain personal information, and that any attachments or enclosures are correct. Take particular care to check email addresses when using a

predictive (auto-complete) email address function, or if an email is going to multiple addressees.

When communicating with someone by email for the first time, a test message should be sent to establish that it is the correct email address before sending any personal information.

Staff must not use their personal email address for work purposes.

Staff should not discuss or reveal personal information which relates to workplace matters in a public setting where it may be seen or overheard.

Processors

Where OSCR uses a third party to process personal information on its behalf, the third party and OSCR must sign a data processing agreement which ensures that they are taking adequate steps to comply with the data protection legislation including Article 28 UK GDPR. OSCR retains legal responsibility for the actions of processors, and so those managing contracts must ensure that all security procedures necessary are specified in the contract, and it is subsequently monitored to ensure that they are in place. Further advice can be obtained via **Corporate**.

Reporting of incidents

A personal information breach means anything that compromises the security, confidentiality, integrity or availability of personal information or the safeguards that protect it. This could include loss or theft of data, (either by loss of a portable device or other media such as an Ironkey) or suspected cyber-attack where there is a loss of data.

All suspected and actual data protection and information security related incidents must be reported immediately on being discovered to the DPO or to the Corporate Team in order to:

- reduce the risk of damage to any affected individuals and our business; and
- allow us to comply with any obligation to notify the ICO or the individuals affected.

OSCR may be required to report breaches to the ICO, so it is imperative that staff report any loss or theft to the DPO as soon as they become aware of the incident. We are legally obliged to notify the ICO of any reportable loss or data breach within 72 hours of discovery, and failure to report could result in a civil penalty.

The rights of individuals

Individuals have a number of rights in terms of their personal information:

- receive certain information about how their information is processed

- request access to their personal information that we hold (subject access request **SAR**)
- request transfer, correction, deletion, restriction of processing
- object to processing (including where this is for direct marketing)
- request a copy of an agreement transferring personal information outside of the United Kingdom
- object to decisions based solely on automated processing, including profiling
- be notified of a personal information breach
- complain to the Information Commissioner, or
- withdraw their consent to processing (if their personal information is processed on the basis consent).

If OSCR receives any communication relating to these rights, they must be forwarded to the DPO immediately. Staff should not respond to the communication or attempt to deal with it without input from the DPO.

International transfers

Any manager or staff member who is required to send personal information in any format to countries outside of the United Kingdom must discuss this with the DPO before any transfer is made.

OSCR makes sure that it only transfers personal data outside of the United Kingdom in compliance with the conditions for transfer set out in chapter five of the GDPR.

New processing activities

It may be necessary for OSCR to carry out a **data protection impact assessment** (**DPIA**) before certain activities are undertaken that involve processing personal information.

A DPIA will consider:

- the impact of the activities
- identify privacy risks and steps to minimise those risks
- evaluate whether the activities are permitted by data protection law.

The following cannot be carried out without first notifying the DPO to determine whether a data protection impact assessment is required:

- process new types of personal information i.e. personal information which has not been collected before.
- process personal information in a new or significantly different way, including via the use of new technologies.
- use personal information for a purpose other than that for which it was collected.

- enter a contract with a third party that involves disclosing or sharing personal information.
- any new or significantly different use of automated processing of personal information to evaluate an individual, for example, to analyse or predict an individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- any new or significantly different use of automated decision-making i.e. where a decision is made on a solely automated basis without meaningful human involvement, and it has a significant effect on individuals.
- any new or significantly different large scale processing of special categories of personal information; or large scale, systematic monitoring of a publicly accessible area. Whether processing is 'large scale' will depend on, for example, the number of individuals, volume of data, range of data, duration of processing, or geographical extent.
- implement significant changes to systems or the business (including new or different technology) which involve processing personal information.
- any new direct marketing activity (including electronic marketing by email, telephone, fax or text message).

Staff awareness and training

All staff must be trained before they can handle personal information in any form in the course of their job. Managers must ensure that their team has received all necessary training.

The Scottish Government and OSCR have a mandatory training programme which includes maintaining awareness of data protection and information handling for all staff. This is carried out by annual completion of e-learning as follows:

- Data Protection e-learning package
- Responsible for Information e-learning package.

Disciplinary issues

A deliberate or reckless breach of the data protection legislation could result in a member of staff facing disciplinary action. Managers must ensure that all staff familiarise themselves with the content of this policy.

Any deliberate or reckless mishandling of personal data by a member of staff may be treated as a disciplinary issue. Staff should be aware that it can be a criminal offence to deliberately or recklessly disclose personal information without the authority of OSCR.