Direct Marketing: Impact of the Privacy and Electronic Communications Regulations (PECRs) and Data Protection

The Privacy and Electronic Communications Regulations cover two main subjects

- **Marketing** - this covers marketing and advertising by electronic means such as by telephone, fax, email, text message and picture (including video) message and by the use of an automated calling system.
- **Use of electronic communications** – this covers the security of public electronic communications services, the confidentiality of communications and restrictions on the processing of certain traffic and location data. The use of cookies is also covered.

In general, the PECRs will only affect University staff/students who are carrying out electronic marketing.

**Direct Marketing**

Direct marketing can cover a range of activities including the offer for sale of goods or services. However, staff should be aware that the ICO considers ‘direct marketing’ to include the promotion of an organisation’s aims and ideals. An example may be a University appeal for funds or support. Best practice dictates that, in general, consent should be obtained before individuals are marketed to.

To conduct a marketing campaign legally, you may have to comply with certain legislation. Depending on how you are marketing you may be affected by the PECRs, Data Protection or both.

**Electronic Marketing**

Marketing using electronic means is covered by the PECRs and may also have a Data Protection element.

To conduct an electronic marketing campaign targeting individuals e.g. to personal email addresses as opposed to generic emails, you must have the consent of the individual. The only exception to this rule is if the ‘soft opt-in’ applies. This applies where:

- you have obtained personal details during a previous sale or transaction AND
- marketing is conducted by the same entity who has dealt previously with the individual AND
- marketing relates to “similar products and services” AND
- an opt-out mechanism is provided at the point of data collection, and is provided with each new communication.

If an individual chooses to opt out of subsequent communications, you MUST adhere to their wishes and no further electronic marketing can be sent.

Anyone sending direct marketing communications using electronic mail must not conceal their identity, and a valid address must be provided for the recipient to opt out of further communications.

There are specific rules regarding the use of automated calling systems. If you intend to use such a system you must check that you are doing so in line with the PECRs.

The Telephone Preference Service (TPS) and Fax Preference Service (FPS) which are operated by the Direct Marketing Association, allow people to register their numbers to opt out of receiving unsolicited calls or faxes. You must not contact individuals or organisations who have registered their numbers with the TPS or FPS unless you have their consent to do so. Further details can be found at: [http://www.tpsonline.org.uk/tps/whatistps.html](http://www.tpsonline.org.uk/tps/whatistps.html) and [http://www.fpsonline.org.uk/fps/](http://www.fpsonline.org.uk/fps/).

**Postal marketing**

Postal marketing may also be used as part of an organisation’s marketing strategy. This type of marketing is not covered by the PECRs. If you are marketing to a named individual then you will have to consider Data Protection. If the individual you are sending your direct marketing to; requests to be removed from your mailing list, you must comply with their request.
The Mailing Preference Service (MPS) was set up by the direct marketing industry to help people who don't want to receive direct marketing. People register their details to prevent further mailings, and several direct marketing codes of practice specify that marketers should check their lists against the MPS file. This does not apply if you have consent to send marketing information to the individual.

Key points to consider when conducting a postal marketing campaign:

- postal marketing campaigns to named individuals should be permission-based
- when obtaining consent you should explain clearly what the contact details will be used for
- provide a simple way for individuals to opt out of marketing messages
- have a system in place for dealing with complaints.

Electronic communications

The PECRs regulate certain types of electronic communications: data which identifies users, their general location, as well as data gathered for billing purposes. This part of the PECRs will only affect the University in a very limited way and is more applicable to large electronic communication service providers. Additional information can be found at: [http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide.aspx](http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide.aspx)

Cookies

Regulation 6 of the PECRs covers the use of electronic communications networks to store information, e.g. using cookies, or gaining access to information stored in the terminal equipment of a subscriber or user.

The University of Strathclyde does not use cookies extensively on its servers at present. Cookies that are used are transient, do not contain any personal information and cannot be used to identify an individual user. Further details about cookies can be found via the ‘Privacy and Cookies’ link: [http://www.strath.ac.uk/privacy/](http://www.strath.ac.uk/privacy/)

PECRs and Data Protection

Regulation 4 of the PECRs states that ‘nothing in these Regulations relieves a person of any of his obligations under the Data Protection Act 1998’.

Depending on the activity you are undertaking, you may have to comply with the PECRs, the Data Protection Act or both.

- If you are using electronic communications, such as email, for a marketing campaign, the PECRs apply.
- If you are using or gathering personal information, the Data Protection Act will apply.
- If you are using electronic communications for marketing to named individuals, both the PECRs and the Data Protection Act will apply.

Enforcement of PECRs

The Privacy and Electronic Communications Regulations and the Data Protection Act are enforced by the ICO. Following the introduction of significant new powers, the Information Commissioner may impose a civil monetary penalty of up to a maximum of £500,000 if a business is found to have committed a very serious breach of the Regulations or the Act. In other cases an Information Notice (requesting further information) or an Enforcement Notice (requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law will be issued. A fine may also be imposed for breach of an Enforcement Notice. The Information Commissioner can also impose civil monetary penalties and conduct audits of processes used University to manage personal data.

Processing Personal Data

The processing of personal data includes but is not limited to:
• Collection, recording or receipt of personal data.
• Storage, backup, filing, or retention of personal data.
• Display, scanning or review of personal data.
• Deletion or destruction of personal data.
• Editing, updating or modification of personal data.
• Copying, transmission, transfer or release of personal data.

Personal data is information that allows an individual to be identified. A name on its own is not necessarily personal data e.g. John Smith. However, if linked with other information e.g. matriculation number or course details, an individual may be identifiable.

Further Information

Further information on the Data Protection Act and the use of personal data can be found at: http://www.strath.ac.uk/dataprotection/

More information on the PECRs can be found on the Information Commissioner's Office (ICO) website: http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications.aspx

Guidance notes on information security can be found at: http://www.strath.ac.uk/is/compliance/recordsmanagement/#d.en.611686

Any queries about the PECRs or Data Protection should be sent to the Information Governance Unit at: dataprotection@strath.ac.uk.