i•creation - Data Protection Policy

Introduction

i•creation takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) very seriously. This policy sets out how the company manages those responsibilities.

i•creation obtains, uses, stores and otherwise processes personal data relating to current and former staff, contractors, website users and contacts, collectively referred to in this policy as data subjects. When processing personal data, the company is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

This policy therefore seeks to ensure that we:

- are clear about how personal data must be processed and the company's expectations for all those who process personal data on its behalf;
- comply with the data protection law and with good practice;
- protect the company's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
- protect the company from risks of personal data breaches and other breaches of data protection law.

The main terms used are explained in the glossary at the end of this policy (Appendix 3).

Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff processing personal data on the Company's behalf must read it. A failure to comply with this policy may result in disciplinary action.

The directors of i•creation are responsible for overseeing this policy.

The company's Data Protection Officer (DPO) is Andy Jackson.

Personal data protection principles

When you process personal data, you should be guided by the following principles, which are set out in the GDPR. The company is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

Those principles require personal data to be:

- processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency).
- collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation).
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data minimisation).
- accurate and where necessary kept up to date (Accuracy). not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation).
- processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality).

Detail on how to achieve this can be found in Appendix 1 & 2.

Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

- where the legal basis of our processing is consent, to withdraw that consent at any time;
- to ask for access to the personal data that we hold;
- to prevent our use of the personal data for direct marketing purposes

- to object to our processing of personal data in limited circumstances
- to ask us to erase personal data without delay:

  a. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

  b. if the only legal basis of processing is consent and that consent has been withdrawn and there is no other legal basis on which we can process that personal data;

  c. if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;

  d. if the data subject has objected to our processing for direct marketing purposes;

  e. if the processing is unlawful.

- to ask us to rectify inaccurate data or to complete incomplete data;
- to restrict processing in specific circumstances e.g. where there is a complaint about accuracy;
- to ask us for a copy of the safeguards under which personal data is transferred outside of the EU;
- the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with the Company; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;
- to prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- to make a complaint to the ICO; and
- in limited circumstances, receive or ask for their personal data to be transferred to a third party (e.g. another company to which a student is transferring) in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed

Requests (including for data subject access – see below) must be complied with, usually within one month of receipt. You must immediately forward any Data Subject Access Request you receive to Andy Jackson. A charge can be made for dealing with requests relating to these rights only if the request is excessive or burdensome.

Accountability

The company must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The company is responsible for, and must be able to demonstrate compliance with, the data protection principles.

We must therefore apply adequate resources and controls to ensure and to document GDPR compliance including:

- appointing a Data Protection Officer (Andy Jackson);
- integrating data protection into our policies and procedures, in the way personal data is handled by us
- training staff on compliance with Data Protection Law and keeping a record accordingly; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

Responsibilities

Company responsibilities

As the Data Controller, the company is responsible for establishing policies and procedures in order to comply with data protection law.

Data Protection Officer responsibilities

The DPO is responsible for:

- advising the company and its staff of its obligations under GDPR
- monitoring compliance with this Regulation and other relevant data protection law, the company's policies with respect to this and monitoring training and audit activities relate to GDPR compliance
- to provide advice where requested on data protection impact assessments
- to cooperate with and act as the contact point for the Information Commissioner's Office
- the data protection officer shall in the performance of his tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Staff responsibilities

Staff members who process personal data about staff or any other individual must comply with the requirements of this policy. Staff members must ensure that:

- all personal data is kept securely;
- no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- personal data is kept in accordance with the company's retention schedule;
- any queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPO;
- any data protection breaches are swiftly brought to the attention of the DPO and the Data Protection Officer and that they support the DPO in resolving breaches;
- where there is uncertainty around a data protection matter advice is sought from the DPO and the Data Protection Officer.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Data Protection Officer.

Third-Party Data Processors

Where external companies are used to process personal data on behalf of the company, responsibility for the security and appropriate use of that data remains with the company.

Where a third-party data processor is used:

- a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- reasonable steps must be taken that such security measures are in place;
- a written contract establishing what personal data will be processed and for what purpose must be set out;
- a data processing agreement, available from the DPO, must be signed by both parties.

Contractors and Short-Term Staff

The company is responsible for the use made of personal data by anyone working on its behalf and should ensure that:

- any personal data collected or processed in the course of work undertaken for the company is kept securely and confidentially;
- all personal data is returned to the company on completion of the work, including any copies that may have been made. Alternatively, that the data is securely

destroyed and the company receives notification in this regard from the contractor or short term / voluntary member of staff;

- the company receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
- any personal data made available by the company, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from the company;
- all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

Reporting a personal data breach

The GDPR requires that we report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly.

We will notify data subjects or the ICO where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, you should immediately contact the Information Compliance Officer, Andy Jackson. You must retain all evidence relating to personal data breaches in particular to enable the company to maintain a record of such breaches, as required by the GDPR.

Limitations on the transfer of personal data

The GDPR restricts data transfers to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit or send that data to a different country or view/access it in a different country.

You may only transfer personal data outside the EU if one of the following conditions applies:

- the European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms. The countries currently approved can be found here:

  https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

- appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- the data subject has provided explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the GDPR including:
- the performance of a contract between us and the data subject
- reasons of public interest,
- to establish, exercise or defend legal claims or
- to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent.

Record Keeping

The GDPR requires us to keep full and accurate records of all our data processing activities. You must keep and maintain accurate corporate records reflecting our processing, including records of data subjects' consents and procedures for obtaining consents, where consent is the legal basis of processing.

These records should include, at a minimum, the name and contact details of the company as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

Records of personal data breaches must also be kept, setting out:

- the facts surrounding the breach
- its effects; and
- the remedial action taken

Training and Audit

We are required to ensure that all company staff undergo adequate training to enable them to comply with data protection law. We must also regularly test our systems and processes to assess compliance.

Sharing Personal Data

In the absence of Consent, a legal obligation or other legal basis of processing, personal data should not generally be disclosed to third parties unrelated to the company.

Some bodies have a statutory power to obtain information (e.g. regulatory bodies such as the Health & Care Professions Council, the Nursing and Midwifery Council, government agencies such as the Child Support Agency). You should seek confirmation of any such power before disclosing personal data in response to a request. If you need guidance, please contact the ICO.

Further, without a warrant, the police have no automatic right of access to records of personal data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. You should seek written assurances from the police that the relevant exemption applies. In all cases where a request is made refer it to the ICO immediately

Important - What this means in practice for the company

- Any personal data in the form of mailing lists provided by customers must be password protected.
- When passing on these data, for instance to a mailing house, passwords must be transmitted in a separate email than the one in which the data is sent.
- Mailing lists must be deleted from the system, and that deletion recorded in the data log held by Andy Jackson, as soon as mailing is complete.
- Photographs and video are important data. Consent forms including GDPR commitments must be completed by everyone who appears in a photograph or video where reasonable. This does NOT include bystanders in public places. In large group shots a single consent from a senior manager
- A review of data held by the company is underway and this policy will be updated in early 2021.

Appendix 1

Principle 1 of GDPR – Processing personal data lawfully, fairly and transparently

Lawfulness and fairness

You may only process personal data fairly and lawfully and for specified purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data for legitimate purposes without prejudicing the rights and freedoms of data subjects. In order to be justified, the company may only process personal data if the processing in question is based on one (or more) of the legal bases set out below. Section 4.3 below deals with justifying the processing of sensitive personal data. Including special category data.

The legal bases for processing non-sensitive personal data are as follows:

1. the data subject has given his or her consent

2. the processing is necessary for the performance of a contract with the data subject (e.g. monitoring academic performance in order to provide the relevant qualification for which the student has enrolled)

3. to meet our legal compliance obligations

4. to protect the data subject's vital interests (i.e. matters of life or death)

5. to pursue our legitimate interests (or another's legitimate interests) which are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The specific legitimate interest or interests that the company is pursuing when processing personal data will need to be set out in relevant Privacy Notices. This ground can only be relied upon for private functions e.g. marketing, fundraising and not for public functions.

You must identify the legal basis that is being relied on for each processing activity, which will be included in the Privacy Notice provided to data subjects.

(a) Consent
You should only obtain a data subject's consent if there is no other legal basis for the processing. consent requires genuine choice and genuine control.

A data subject consents to processing of his/her personal data if he/she indicates agreement clearly either by a statement or positive action to the processing. Silence, pre-ticked boxes or inactivity are therefore unlikely to be sufficient. If consent is

given in a document that deals with other matters, you must ensure that the consent is separate and distinct from those other matters.

Data subjects must be able to withdraw consent to processing easily at any time. withdrawal of consent must be promptly honoured. consent may need to be renewed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented, or if the consent is historic.

You will need to ensure that you have evidence of consent and you should keep a record of all consents obtained so that we can demonstrate compliance.

Consent is required for some electronic marketing and some research purposes.

(b) Legal bases for Processing Sensitive Personal Data, including Special Category Data
Special Category Personal Data is data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs,
- trade union membership,

It also includes the processing of:

- genetic data
- biometric data for the purpose of uniquely identifying a natural person,
- data concerning health
- data concerning a natural person's sex life or sexual orientation

Personal data relating to criminal convictions and offences including the alleged commission of offences or proceedings for offences or alleged offences should be treated in the same way to special category data.

The processing of sensitive personal data by the company must be based on one of the following (together with one of the legal bases for processing non-sensitive personal data as listed above):

- the data subject has given explicit Consent (requiring a clear statement, not merely an action)
- the processing is necessary for complying with employment law;

- the processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving Consent;
- the processing relates to personal data which are manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary for reasons of substantial public interest (provided it is proportionate to the particular aim pursued and takes into account the privacy rights of the data subject)
- the processing is necessary for the purposes of preventive or occupational medicine, etc. provided that it is subject to professional confidentiality
- the processing is necessary for reasons of public interest in the area of public health, provided it is subject to professional confidentiality;
- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes if it is subject to certain safeguards (i.e. pseudonymisation or anonymisation where possible, the research is not carried out for the purposes of making decisions about particular individuals (unless it is approved medical research) and it must not be likely to cause substantial damage/distress to an individual and is in the public interest).

Examples of sensitive personal data processed by the company will include:

- details of relevant unspent convictions for the purposes of assessing suitability for employment
- unspent convictions or allegations of sexual misconduct for staff and disciplinary purposes
- health data for the purposes for assessing eligibility to undertake relevant professional programmes, assessing fitness to engage in company activities or for assessing fitness to work
- details of disability for the purposes of assessing and implementing reasonable adjustments to the company's policies, criteria or practices
- details of racial/ethnic origin, sexual orientation, religion/belief for the purposes of equality monitoring

Processing sensitive personal data represents a greater intrusion into individual privacy than when processing non-sensitive personal data. You must therefore take special care when processing sensitive personal data and ensure that you comply with the data protection principles (as set out in the main body of this policy) and with this policy, in particular in ensuring the security of the sensitive personal data.

Transparency (notifying data subjects)

Under the GDPR the company is required to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. That information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand what happens to their personal data.

Whenever we collect personal data directly from data subjects, for example for the recruitment and employment of staff, at the time of collection we must provide the data subject with all the prescribed information which includes:

- Company's details
- Contact details of DPO
- Purposes of processing
- Legal basis of processing
- Where the legal basis is legitimate interest, identify the particular interests (e.g. marketing, fundraising)
- Where the legal basis is consent, the right to withdraw
- Where statutory/contractual necessity, the consequences for the Data Subject of not providing the data of non-provision

When personal data is collected indirectly (for example, from a third party or publically available source), you must also provide information about the categories of personal data and any information on the source. The data subject must be provided with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

Appendix 2

Principle 2 of GDPR - Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot therefore use personal data for entirely new, different or incompatible purposes from those disclosed when it was first obtained unless you have informed the data subject of the new purposes. Where the further processing is not based on the data subject's Consent or on a lawful exemption from data-protection law requirements, you should assess whether a purpose is incompatible by taking into account factors such as:

- the link between the original purpose/s for which the personal data was collected and the intended further processing
- the context in which the personal data has been collected – in particular the Company-data subject relationship. You should ask yourself if the data subject would reasonably anticipate the further processing of his/her personal data
- the nature of the personal data in particular whether it involves special categories of personal data (i.e. sensitive) or personal data relating to criminal offences/convictions
- the consequences of the intended further processing for the data subjects
- the existence of any appropriate safeguards e.g. encryption or pseudonymisation.

Principle 3 of the GDPR – Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You should not therefore amass large volumes of personal data that are not relevant for the purposes for which they are intended to be processed. Conversely, personal data must be adequate to ensure that we can fulfil the purposes for which it was intended to be processed.

You may only process personal data when performing your job duties requires it and you should not process personal data for any reason unrelated to your job duties.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention policy and schedule.

Principle 4 of the GDPR – Accuracy

Personal data must be accurate and, where necessary, kept up to date. You should ensure that personal data is recorded in the correct files.

Incomplete records can lead to inaccurate conclusions being drawn and in particular, where there is such a risk, you should ensure that relevant records are completed.

You must check the accuracy of any personal data at the point of collection and at regular intervals thereafter. You must take all reasonable steps to destroy or amend inaccurate records without delay and you should up-date out-of-date personal data where necessary (e.g. where it is not simply a pure historical record).

Where a data subject has required his/her personal data to be rectified or erased, you should inform recipients of that personal data that it has been erased/rectified, unless it is impossible or significantly onerous to do so.

Principle 5 of the GDPR – Storage limitation

You must not keep personal data in a form that allows data subjects to be identified for longer than needed for the legitimate educational/research or Company business purposes or other purposes for which the Company collected it. Those purposes include satisfying any legal, accounting or reporting requirements. Records of personal data can be kept for longer than necessary if anonymised.

You will take all reasonable steps to destroy or erase from the Company's systems all personal data that we no longer require in accordance with all relevant Company records retention schedules and policies. The Company has a document retention policy.

You will ensure that data subjects are informed of the period for which their personal data is stored or how that period is determined in any relevant Privacy Notice.

Principle 6 of the GDPR – Security, Integrity and Confidentiality

The company is required to implement and maintain appropriate safeguards to protect personal data, taking into account in particular the risks to data subjects presented by unauthorised or unlawful processing or accidental loss, destruction of, or damage to their personal data. Safeguarding will include the use of encryption and pseudonymisation where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorised to use personal data have access to it), integrity and availability of the personal data.

You are also responsible for protecting the personal data that you process in the course of your duties. You must therefore handle personal data in a way that guards against accidental loss or disclosure or other unintended or unlawful processing and in a way that maintains its confidentiality. You must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

You must comply with all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction.

You must comply with all applicable aspects of our Information Security Policy, and comply with and not attempt to circumvent the administrative, physical and technical safeguards we

implement and maintain in accordance with the Data Protection Law standards to protect personal data.

You may only transfer personal data to third-party service providers (i.e. data processors) who provide sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Law and who agree to act only on the company's instructions. Data processors should therefore be appointed subject to the company's standard contractual requirements for data processors.