Ironclad Creative CIC - Data Protection Policy (April 2021)

Data Protection: Introduction

Ironclad Creative CIC ("IC") collects data from our members, service users and participants who attend our training courses, use our online community network and attend events. We also collect data from staff, contractors and suppliers.

This Policy sets out our procedures for the collection, storage, use and sharing of personal data and data for electronic business to business communications.

The Policy will be reviewed by IC's board every 3 years, or earlier if there are changes to legislation and/or to IC's use of data . Current relevant legislation is: the Data Protection Act ("the Act"), the General Data Protection Regulations ("the GDPR") and the Privacy and Electronic Communications Regulations ("PECR").

What data is relevant?

Data Protection legislation is concerned with the use of personal data, held on electronic systems, in paper filing and online identifiers such as location data and cookies.

Personal data is defined by the Information Commissioners Office ("the ICO") as data that relates to a living individual who can be identified –

• from that data, or

• from that data and other information in the possession of (or likely to come into the possession of) the data controller e.g: expressions of opinion about an individual.

• from codified records that do not identify individuals by name but, for example, bear unique reference numbers that can be used to identify the individuals concerned.

Special categories of personal data means information that could be used in a discriminatory way, so needs to be treated with greater care than other personal data, i.e: information about:-

• race or ethnic origin

• political opinions

• religious beliefs or other beliefs of a similar nature,

• trade union membership

• physical or mental health or condition,

• sexual life,

• commission or alleged commission by the data subject of any offence, or

• any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Definitions of data and people:

A data subject: Anyone whose data is processed.

A data controller: The organisation/ person who decides how and personal data is/will be, processed. Data controllers will usually be organisations, but can be individuals, for example self-employed consultants.

A data processor: Any person (other than an employee of the data controller) who processes the data on behalf of the data controller, e.g: external payroll service providers.

Consent

In line with the GDPR we will ensure that when we process personal data we have the data subject's consent and that the data subject has been made aware that they have the right to withdraw their consent. Consent must be:-

• Specific to the purpose for which we are using the data.

• Unambiguous

• Active not implied: Silence is not consent; pre-ticked boxes, inactivity, failure to opt-out or passive acquiescence will not constitute valid consent.

• Freely given: Consent will not be valid if the data subject does not have a genuine and free choice or cannot refuse or withdraw consent without detriment.

Ways in which we may ask for consent include:-

• Written consent;

• Ticking a box on a web page;

• Choosing technical settings in an app;

• Verbal consent (which is then recorded in writing)

• Any other statement/conduct that clearly indicates (in this context) the data subject's acceptance of the proposed processing of personal data e.g: cookie acceptance.

In line with PECR we will not contact individuals for direct marketing purposes by email, the internet, phone, fax or any new electronic systems that may be introduced without prior consent. (NB: Business to business communications to generic addresses such as “admin@” “info@” do not require consent.)

We provide opt-out opportunities in every mailing to ensure compliance with the principle that data held should be accurate and up to date.

All our mailings make it clear who the sender is, so the recipient’s ability to opt out is viable.

Our website makes it clear we use cookies to collect details of visitors to our website and gives them an opportunity to refuse their operation.

Who does Ironclad Creative CIC collect/process/store data from?

• **Community members**: Current, past and potential – this will include personal data around name, geographical residence, email and creative discipline. Participants are also asked to fill out separate and optional monitoring forms around special categories of personal information.

• **Training participants/facilitators (contractors / freelance):** Details of attenders and trainers – this is likely to involve personal data around names, geographical residence. Participants are also asked to fill out separate and optional monitoring forms around special categories of personal information.

• **Staff recruitment** – this will be personal data.

• **Staff records** - this will be personal and some may be special category data.

How do we deal with data?

Community members joining The Ironclad Hub: When our community members join The Ironclad Hub they are joining the Mighty Network platform, and as such agree to give us, as Hosts, personal information, as per the privacy policy of Mighty Networks. https://www.mightynetworks.com/privacy-policy

Community members & training participants interaction:

We use Mighty Networks, Mailchimp, Eventbrite, Paypal, Ko-fi, Facebook, Instagram, Twitter and G-suite to interact with our community members and training participants/facilitators. Each of these sites have data protection / privacy policies in place and require users to opt in.

When we collect data from data subjects in person or via the above means (for feedback surveys and/or mailing list sign up, for example) we we make it clear that we do not share data with any third parties and that applicants are given the choice to opt in to:-

• IC processing any personal data they may provide.

• IC using their data for marketing purposes, i.e to send news and training and events information.

• IC using their data for funding purposes, i.e to use anonymised data around diversity for funding applications/reportage (see: Diversity monitoring).

It also includes a statement that we do not sell, trade or rent personal data to others, information about the right to be forgotten and information on how to make a data subject request.

Staff/contractor/freelancer recruitment: The IC application form will include a declaration that states that the applicant understands that their personal data is being processed solely for the purpose of this specific job application and that sensitive data in the Equal Opportunities Monitoring form is processed

anonymously. It also states that we do not sell, trade or rent personal data to others, that application material will be destroyed after 12 months and information on how to make a data subject request. Rejection letters shall offer the option to have personal data kept on IC records for more than a year if they want to be considered if another suitable vacancy arises. This must be an opt in tick box that can be returned to IC by post or email.

Diversity monitoring: These forms contain special category data by definition, however they are anonymous, separated from other survey / feedback forms.

[Note: we currently have no PAYE staff and this policy section for information only]

Staff records (not contract / freelance): Our staff contract reflects the fact that the law allows us to collect some data about employees and that employees have the right to access this. The relevant clause says

Data Protection: For the purposes of administration, such as payroll and pension auto-enrolment, it is necessary for Ironclad Creative to hold and sometimes disclose certain personal data about employees.

i) Any data IC holds about the Employee will only be held for so long as the Employee works for IC, unless IC is required to hold it for longer in order to comply with the law. IC shall take every care to ensure personal data is held securely and in confidence.

ii) The Employee has the right to inspect data that IC holds about her and, if necessary, update that data. Normally inspection of files can be within 10 working days of a request.

iii) If the Employee's personal information changes at any time, she should inform her line manager as soon as possible to ensure that the information remains accurate.

Deletion of data: Data subjects have the right to request to be "forgotten", Ironclad will delete records in line with GDPR as follows:-

• When processing can cause substantial damage or distress.

• Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

• When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

• If the personal data was unlawfully processed.

If personal data being erased has been disclosed to third parties we will inform them about the erasure, unless it is impossible or involves disproportionate effort.

If personal information has been processed online, for example on social networks, forums or websites we will inform any other organisations who are involved to erase links to, copies or replication of “forgotten” personal data.

IC will not always delete records, a request to be forgotten can be refused where data has been processed:

• To exercise the right of freedom of expression and information;

• To comply with a legal obligation for the performance of a public interest task or exercise of official authority.

• For public health purposes in the public interest;

• For archiving purposes in the public interest, scientific research historical research or statistical purposes; or

• For the exercise or defence of legal claims.

Data Protection Officer

IC does not need a designated Data Protection Officer under the GDPR, however, the Co-founding Producer (Michelle Allen) is responsible for ensuring Data Protection Compliance, working with the Co-founding Director (Andrew Allen) and the Non-Executive Directors as appropriate.

Appendix A The principles of good data protection practice

IC processes data in line with the Act, which says that:

• Personal data shall be processed fairly and lawfully

• Personal data shall be obtained only for specified, lawful purposes and shall not be further processed in any manner incompatible with such purpose(s).

• Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

• Personal data shall be accurate and, where necessary, kept up to date.

• Personal data processed for any purpose(s) shall not be kept for longer than is necessary.

• Personal data shall be processed in accordance with the rights of data subjects under the Act.

• Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of or damage to, personal data.

• Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix B Statutory Data Retention Periods

Accident books, accident records/reports: 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).

Accounting records: 3 years for private companies, 6 years for public limited companies.

Income tax and NI returns, income tax records and correspondence with HMRC: Not less than 3 years after the end of the financial year to which they relate.

Medical records and details of biological tests under the Control of Lead at Work Regulations: 40 years from the date of the last entry.

Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH): 40 years from the date of the last entry.

Medical records under the Control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos and medical examination certificates: (medical records) 40 years from the date of the last entry; (medical examination certificates) 4 years from the date of issue.

Medical records under the Ionising Radiations Regulations 1999: until the person reaches 75 years of age, but in any event for at least 50 years.

Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH): 5 years from the date on which the tests were carried out.

Records relating to children and young adults: until the child/young adult reaches the age of 21.

Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity: 6 years from the end of the scheme year in which the event took place.

Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence: 3 years after the end of the tax year in which the maternity period ends.

Wage/salary records (also overtime, bonuses, expenses): 6 years.

National minimum wage records: 3 years after the end of the pay reference period following the one that the records cover.

Records relating to working time: 2 years from date on which they were made.

Appendix C Recommended non-Statutory Data Retention Periods

Application forms and interview notes (for unsuccessful candidates): 6 months to a year. Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants documents will be transferred to the personnel file in any event.

Assessments under health and safety regulations and records of consultations with safety representatives and committees: permanently.

Inland Revenue/HMRC approvals: permanently.

Money purchase details: 6 years after transfer or value taken.

Parental leave: 5 years from birth/adoption of the child or 18 years if the child receives a disability allowance.

Pension scheme investment policies: 12 years from the ending of any benefit payable under the policy.

Pensioners' records: 12 years after benefit ceases.

Personnel files and training records (including disciplinary records and working time records): 6 years after employment ceases.

Redundancy details, calculations of payments, refunds, notification to the Secretary of State: 6 years from the date of redundancy

Senior executives' records (that is, those on a senior management team or their equivalents): permanently for historical purposes.

Statutory Sick Pay records, calculations, certificates, self-certificates: The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 abolished the obligation on employers to keep these records, however, employers still have to keep sickness records to best suit their business needs. It is advisable to keep records for at least 3 months after the end of the period of sick leave in case of a disability discrimination claim. However if there were to be a contractual claim for breach of an employment contract it may be safer to keep records for 6 years after the employment ceases.

Trade union agreements: 10 years after ceasing to be effective.

Trustees' minute books: permanently.

Works council minutes: permanently.