Data Retention and Erasure Policy

Policy Statement

hi-impact consultancy ltd recognises and understands that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the organisation.

Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles. hi-impact only ever retains records and information for legitimate business reasons and use and we comply fully with the UK data protection laws and guidance.

Effective and adequate records and data management is necessary to: -

- Ensure that the business conducts itself in a structured, efficient and accountable manner
- Ensure that the business realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Support core business functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes
- Meet legislative, statutory and regulatory requirements
- Deliver services to, and protect the interests of, employees, clients and stakeholders in a consistent and equitable manner
- Assist in document policy formation and managerial decision making
- Provide continuity in the event of a disaster or security breach
- Protect personal information and data subject rights
- Avoid inaccurate or misleading data and minimise risks to personal information
- Erase data in accordance with the legislative and regulatory requirements

Purpose

The purpose of this policy is to set out the length of time that hi-impact's records should be retained, the processes for disposing of records, how hi-impact provides a structured and compliant data and records management system. We define 'records' as all documents, regardless of the format; which facilitate business activities, and are thereafter retained to provide evidence of transactions and functions.

Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

Scope

This policy applies to all staff within hi-impact (*meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with hi-impact in the UK or overseas*). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

Personal Information and Data Protection

hi-impact needs to collect personal information about the people we employ, work with or have a business relationship with, to effectively and compliantly carry out our everyday business functions and activities, and to provide our products and services. This information can include (but is not limited to), name, address, email address, data of birth, IP address, national insurance number, private and confidential information, sensitive information and bank details. From time to time we receive childrens data to setup platforms and applications, this data is used and the immediately deleted.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the General Data Protection Regulation, UK data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Retention Policy and processes comply fully with the GDPR's fifth Article 5 principle: - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

Objectives

A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions. It is hi-impact's objective to implement the necessary record,s management procedures and systems which assess and manage the following processes: -

- The creation and capture of records
- Compliance with legal, regulatory and contractual requirements
- The storage of records
- The protection of record integrity and authenticity
- The use of records and the information contained therein
- The security of records
- Access to and disposal of records

Records contain information that are a unique and invaluable resource to hi-impact and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

hi-impact's objectives and principles in relation to Data Retention are to: -

- Ensure that hi-impact conducts itself in an orderly, efficient and accountable manner
- Support core business functions and providing evidence of compliant retention, erasure and destruction
- Develop and maintain an effective and adequate records management program to ensure effective archiving, review and destruction of information
- Only retain personal information for as long as is necessary
- Comply with the relevant data protection regulation, legislation and any contractual obligations
- Ensure the safe and secure disposal of confidential data and information assets
- Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each bodies rules or terms
- Ensure that no document is retained for longer than is legally or contractually allowed
- Mitigate against risks or breaches in relation to confidential information

Guidelines and Procedures

hi-impact manage records efficiently and systematically, in a manner consistent with the GDPR requirements. Records management training is mandatory for all staff as part of hi-impact's induction process and this policy is widely disseminated to ensure a standardised approach to data retention and records management.

Records will be created, maintained and retained to provide information about, and evidence of hi-impact's transactions, customers, employment and activities. Retention schedules will govern the period that records will be retained.

It is our intention to ensure that all records and the information contained therein is: -

- Accurate - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- Accessible - records are always made available and accessible when required (*with additional security permissions for select staff where applicable to the document content*)
- Complete - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- Compliant - records always comply with any record keeping legal and regulatory requirements
- Monitored – staff, company and system compliance with this Data Retention Policy is regularly monitored to ensure that the objectives and principles are being

complied with at all times and that all legal and regulatory requirements are being adhered to

Retention Periods and Protocols

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All company and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

For all data and records obtained, used and stored within hi-impact, we: -

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
- Establish periodical reviews of data retained
- Establish and verify retention periods for the data, with special consideration given in the below areas:
    - the requirements of hi-impact
    - the type of personal data
    - the purpose of processing
    - lawful basis for processing
    - the categories of data subjects
- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, hi-impact will identify the criteria by which the period can be determined and provide this to the data subject on request

Designated Owners

All systems and records have designated owners throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, business area and level of access to the data required. The designated owner is recorded on the Retention Register and is fully accessible to all employees. Data and records are never reviewed, removed, accessed or destroyed without the prior authorisation and knowledge of the designated owner.

Document Classification

We carry out regular Information Audits which enable us to identify, categorise and record all personal information obtained, processed and shared by our company in our capacity as a controller and processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?

- Retention periods
- Access level (i.e. full, partial, restricted etc.)

Our information audits and registers enable us to assign classifications to all records and data, thus ensuring that we are aware of the purpose, risks, regulations and requirements for all data types. We utilise 5 main classification types: -

1. Unclassified - information not of value and/or retained for a limited period where classification is not required or necessary
2. Public - information that is freely obtained from the public and as such, is not classified as being personal or confidential
3. Internal - information that is solely for internal use and does not process external information or permit external access
4. Personal - information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws
5. Confidential - private information or systems that must be secured at the highest level and are afforded access restrictions and high user authentication

The classification is used to decide what access restriction needs to be applied and the level of protection afforded to the record or data.

Storage and Access of Records and Data

Documents are grouped together by category and then in clear date order when stored and/or archived. Documents are always retained in a secure location, with authorised personnel being the only ones to have access. Once the retention period has elapsed, the documents are either reviewed, archived or confidentially destroyed dependant on their purpose, classification and action type.

Expiration of Retention Period

Once a record or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR requirements or to archive records for a further period.

Destruction and Disposal of Records and Data

All information of a confidential or sensitive nature on paper or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

hi-impact is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

Paper Records

Due to the nature of our business, hi-impact retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner.

Employee shredding machines are made available throughout a number of offices.

Electronic and IT Records and Systems

hi-impact uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner. hi-impact use a third party disposal company to dispose of any IT equipment for hi-impact's assets and contracted schools.

The deletion of electronic records must be organised in conjunction with the technical department who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner and Senior Data Practitioner to maintain an effective and up to date register of destroyed records.

Only the Technical Department can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department personally. Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

In all disposal instances, for hi-impact or on behalf of clients, the Technical Department must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the Technical Department is responsible for liaising with the Information Asset Owner and providing the required information for them to update the Information Asset Register for the asset that has been removed.

It is the explicit responsibility of the disposal company to ensure that all relevant data has been sufficiently removed from the IT device. Following disposal hi-impact will receive a disposal certificate and reference number which is recorded by hi-impact.

Erasure

In specific circumstances, data subjects' have the right to request that their personal data is erased, however hi-impact recognise that this is not an absolute 'right to be forgotten'. Data subjects only have a right to have personal data erased and to prevent processing if one of the below conditions applies: -

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

- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Where one of the above conditions applies and hi-impact received a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out by the Data Protection/ Request Management Officer with the support of the Senior Data Practitioner and Organisation Measure Officer. This should be done in conjunction with the department manager and technical department to ensure that all data relating to that individual has been erased.

These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed: -

1. The request is allocated to the Data Protection/Request Management Officer and recorded on the Erasure Request Register
2. The Senior Data Practitioner and Organisational Measures Officer will support with the locating of all personal information relating to the data subject and review it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
    1. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    2. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    3. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
    4. the personal data has been unlawfully processed
    5. the personal data must be erased for compliance with a legal obligation
    6. the personal data has been collected in relation to the offer of information society services to a child
4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The Data Protection/Request Management Officer writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure

6. Where hi-impact has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. *Such refusals to erase data include: -*

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

Special Category Data

In accordance with GDPR requirements and Schedule 1 Part 4 of The Data Protection Bill, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc.

Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted below.

Compliance and Monitoring

hi-impact are committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention.

Responsibilities

Heads of departments and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure that the records created, received and controlled within the purview of their department, and the systems (electronic or otherwise) and procedures they adopt, are managed in a way which meets the aims of this policy.

Our GDPR Compliance Team will be involved in any data retention processes and record of all archiving and destructions must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with hi-impact’s protocols.

Retention Periods

Employment records			
Record	**Recommended retention period**	**Storage format**	**Reference**
Rejected job applicant records, including: ● contact details ● application letters or forms ● CVs ● references ● certificates of good conduct ● interview notes	1 year Application forms should give applicants the opportunity to object to their details being retained	Paper or electronic	https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf Equality Act 2010, s 123
Application records of successful candidates, including: ● application letters or forms ● copies of academic and other training received ● references correspondence concerning employment ● CVs ● interview notes and evaluation forms	Six years after employment ceases	Paper or electronic	Limitation Act 1980 (LA 1980), s 5
Criminal records information: ● criminal records requirement assessments for a particular post ● criminal records information forms ● Disclosure and Barring Service (DBS) check forms ● DBS certificates	Criminal records requirement assessments for a particular post— 12 months after the assessment was last used All other information in this category—as soon as practicable after the check has been completed and the outcome recorded (ie whether satisfactory or not) unless, in exceptional circumstances, [the Data Protection Officer assesses that it is clearly	Paper or electronic	DBS guidance for employers: Duration of criminal record check validity https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

	relevant to the ongoing employment relationship in which case, six months If Data Protection Officer considers it necessary to keep the information for longer than six months, the DBS should be consulted.		
Employment contracts, including: ● Personnel and training records ● Written particulars of employment ● Changes to terms and conditions	Six years after employment ceases, unless document executed as a deed, in which case 12 years after employment ceases.	Paper or electronic	LA 1980, ss 5, 8
Directors' service contracts and any variations	Six years from termination or expiry of the contract, unless executed as a deed, in which case 12 years from termination or expiry	Paper or electronic	LA 1980, ss 5, 8 Companies Act 2006, ss 227 and 228
Copies of identification documents (eg passports)	Not less than two years from date of termination of employment	Paper or electronic	Immigration (Restrictions on Employment) Order SI 2007/3290, Art 6(1)(b)
Identification documents of foreign nationals (including right to work)	Not less than two years from date of termination of employment	Paper or electronic	Immigration (Restrictions on Employment) Order SI 2007/3290, art 6(1)(b)
Records concerning a temporary worker	Six years after employment ceases	Paper or electronic	LA 1980, s 5
Employee performance and conduct records, including: ● probationary period ● reviews ● review meeting and assessment interviews ● appraisals and evaluations	Six years after employment ceases	Paper or electronic	LA 1980, s 5

• promotions and demotions			
Records relating to and/or showing compliance with Working Time Regulations 1998 including: • registration of work and rest periods • working time opt-out forms	Two years from the date on which the record was made	Paper or electronic	Working Time Regulations 1998, SI 1998/1833, reg 9
Redundancy records	Six years from date of redundancy	Paper or electronic	LA 1980, s 5
Annual leave records	Six years after the end of each tax year	Paper or electronic	LA 1980, s 5
Parental leave records	Six years after the end of each tax year	Paper or electronic	LA 1980, s 5
Sickness records	Six years after the end of each tax year	Paper or electronic	LA 1980, s 5
Records of return to work meetings following sickness, maternity etc	Six years the end of each tax year	Paper or electronic	LA 1980, s 5

Payroll and salary records			
Record	**Recommended retention period**	**Storage format**	**Reference**
Records for the purposes of tax returns including wage or salary records, records of overtime, bonuses and expenses	Six years	Paper or electronic	Taxes Management Act, 1970 s 12B Finance Act 1998, Schedule 18, para 21
Pay As You Earn (PAYE) records, including: wage sheets deductions working sheets calculations of the PAYE income of employees and relevant payments	Three years	Paper or electronic	Income Tax (Pay As You Earn) Regulations 2003, SI 2003/2682, reg 97
Income tax and NI returns, income tax records and correspondence with HMRC	Three years after the end of the financial year to which they relate	Paper or electronic	Income Tax (Employments) Regulations 1993, SI 1993/744, reg 55
Records demonstrating compliance with national	Three years beginning with the day upon which the	Paper or electronic	National Minimum Wage Regulations 2015, SI 2015/621, reg 59

minimum wage requirements	pay reference period immediately following that to which they relate ends		
Details of benefits in kind, income tax records (P45, P60, P58, P48 etc), annual return of taxable pay and tax paid	Six years (but general time limit under the TMA 1970 is reducing to four years from 1 April 2012)	Paper or electronic	Taxes Management Act 1970
Employee income tax and national insurance returns and associated HMRC correspondence	Three years from end of tax year to which they relate	Paper or electronic	Income Tax (Pay as You Earn) Regulations 2003, SI 2003/2682, reg 97
Statutory sick pay (SSP) records	Three years after the end of the tax year to which they relate	Paper or electronic	The requirement to maintain SSP records for three years after the end of the tax year to which they relate was revoked in 2014, but an employer may still be required by HMRC to produce such records as are in his possession or power which contain, or may contain, information relevant to satisfy HMRC that statutory sick pay has been and is being paid. The Statutory Sick Pay (General) Regulations 1982, SI 1982/894, reg 13(A)
Wage or salary records (including overtime, bonuses and expenses)	Six years	Paper or electronic	Taxes Management Act 1970, s 43
Records relating to hours worked and payments made to workers	Three years	Paper or electronic	National Wage Act 1998, s 9 The National Wage Regulations 1999, reg 38
Statutory maternity, paternity and shared parental pay records, calculations, certificates or other evidence	Three years after the end of the tax year in which the period of statutory pay ends	Paper or electronic	Statutory Maternity Pay (General) Regulations 1986, SI 1986/1960, reg 26

Health and safety records			
Record	**Recommended retention period**	**Storage format**	**Reference**
Records of reportable injuries, diseases or dangerous occurrences ● reportable incidents ● reportable diagnosis	Three years from date of the entry	Paper or electronic	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013

• injury arising out of accident at work (including [*insert organisation's name*]'s accident book)			(RIDDOR 2013), SI 2013/1471, reg 12

ıternal Data Retention Periods

Record	**Retention period**
Emails	1 year for all staff 2 years for management
Photographs with consent	1 year unless approved by client for marketing purposes
Marketing/ feedback/ survey contact details	1 year with consent. At 1 year resend reminder to continue receiving updates.
Videos with consent	1 year unless approved by client for marketing purposes
Personal Information from clients to create log in details	Immediately after the information is used.
Workshop photographs	At the end of every term.