Ixion Group Policy & Procedure

Data & Document Retention and Disposal

Policy Statement

Ixion is responsible for handling numerous items of classified information in both electronic and paper form. Ixion complies with the General Data Protection Regulations (GDPR), the records retention requirements of regulatory bodies and the contractual requirements of commissioning bodies.

Ixion recognises also that it has a duty of care towards its clients and employees to safeguard personal data from loss, damage or disclosure. Therefore, given that a significant proportion of Ixion records are or are related to personal information, the spirit of the six GDPR Principles are applied to all records created and retained by Ixion.

Our policy is to

1) retain records and information in all its forms securely
2) retain information for no longer than is required under statute, contract or other legal obligation
3) retain no more information than is required under statute, contract or other legal obligation
4) ensure that the integrity of the information is preserved
5) preserve information in an accessible form for future reference and audit
6) destroy all records and data that are no longer required
7) not store personal data in a country or territory outside the European Economic Area, with the exception of the US if the recipient of the data has signed up to the Privacy Shield Framework designed by the U.S. Department of Commerce and the European Commission.

Ixion shall apply the principle that electronic data and documents will be retained as if they were paper documents. Therefore, any electronic data or files that fall into one of the categories on the below schedule will be maintained for the prescribed period. If a piece of electronic data is required to be retained indefinitely, or retained beyond the designated retention period, (e.g. an e-mail message), the message should be printed in hard copy and kept in the appropriate physical document file.

Why we need this policy

- To ensure that Ixion maintains electronic data records appropriately
- To demonstrate to all stakeholders that Ixion recognises the importance of data retention in combination with good records management
- To ensure compliance with legislation, including General Data Protection Regulation and with contractual requirements

- To expedite and facilitate any future criminal or civil investigation where records held by the Trust may be required as evidence.

Communication

This policy will be communicated to all staff through staff induction and periodic refresher training. All staff will be notified via email and through staff meetings of any updates to this policy.

Associated Policies

This Policy and associated procedures should be read in conjunction with the following Policies:

- Document Classification and Control
- Data Protection and the General Data Protection Regulations (GDPR)
- Information Assurance and Security
- Discipline and Dismissal

Storage

Data and documents are stored with appropriate security arrangements in place to avoid potential misuse or loss. The frequency of access to the documents, and whether a document is active or no longer being used, determines the appropriateness of where the document is stored. The sensitivity and confidentiality of the information determines the degree of security surrounding the method of storage. Storage options include:

- locked pedestals
- locked filing cabinets – often within a secure room
- in password protected files on local IT systems
- on data systems encrypted to FIPS 140-2 standards
- on commissioner/prime contractor secure data systems
- scan/upload facilities to secure IT systems

Where documents can be scanned and uploaded to secure IT systems this should be carried out in line with the relevant guidance from the system owner. Such records are usually stored on a specified data carrier, and certified as being copies of the original, meeting national standards and being auditable.

Documents that become inactive but are required to be kept for auditing /legislative purposes are archived with a secure storage provider. In the case of subcontract arrangements, documents due to be archived may be transferred to the ownership of the prime contractor in line with contractual arrangements.

Ixion's Electronic Data Storage

Ixion's live data is retained on company-owned physical self-encrypting Storage Area Networks (SAN) encrypted to FIPS 140-2 standards. Though use of VPLEX (An EMC innovation) the data is replicated over a secure MPLS network to a second site. The production SANs are based within secure locked racks with no less than a secure tier 3+ data centre (DC) and only accessed by certified, screened and entrusted individuals. Ixion regularly backs up its live data to a second set of backup SANs using FIPS 140-2 software encryption via the secure MPLS network through the use of Veeam.

Retention Periods

The following minimum retention periods shall apply for data.

File Category	Item	Minimum Retention Period
Contract Documentation (exc. personal data processed as part of contracts with commissioning bodies)	Contracts	6 years from contract expiry
	Deeds	12 years
	Property / Land Conveyances	Permanent (and/or paper document)
	Funding Agreements	Specific to each agreement
Corporate Documentation	Company formation documents	Permanent (and/or paper document)
	Register of directors and company secretaries	Permanent (and/or paper document)
	Minutes of board meetings and general meetings	10 years from meeting
	Accounting records, banking records and books of accounts	3 years from creation
	Audits	5 years from date of auditors report
Tax Documentation	Corporation Tax	6 years following end of relevant accounting period
	VAT	
	Stamp Duty Land Tax	
Employment Documentation (N.B. See below re HMPPS	PAYE Records	3 years from end of financial year
	Records of National Insurance contributions	3 years from end of year contribution was payable

document retention)		
	Maternity, paternity and adoption payment records	3 years from end of tax year payment was made
	Sickness records	3 years from end of tax year in which created
	General Employee history / employment records (Inc. unfair dismissal, discrimination, statutory redundancy pay, equal pay claim)	6 month from termination of employment
	Employee history / employment records – Breach of employment	6 years of the event constituting the alleged breach
	Employee records associated with Tax	6 years following end of relevant accounting period
Health and Safety Documentation	Health and safety policy	Permanent (and/or paper document)
	Risk assessment reports	Permanent (and/or paper document)
	Injury records and accident books	3 years from the accident date
Specific Electronic files (Excl. Client Data)	Emails	6 years from sending date unless specifically identified in categories above
	General operational files and staff functional data (databases, word documents, spreadsheets, slides, plans, etc.	No retention period unless defined by the specific business need
	Electronic communications including instant messaging, tweets, posts, news articles, intranet site, eLearning	No retention period unless specifically covered in categories above
	Video: live, recorded, streamed	
	Telephone calls, contact centres, live voice, recorded voicemails, voice messaging, etc.	No retention period
HMPPS CFO Records	Financial records Incident records Complaint records	12 years beyond project end date

	Record of visitors Personnel records Staffing details Administrative records	
ESF Evidence for all projects funded by ESF during the funding period 2014-2020	All contractual records	To be retained until 31 December 2030.

Where it is not practical to segregate and manage specific data types uniquely, then a blanket 7 year policy shall be applied to all data with a prescribed retention period of 6 years or less.

Client / Customer Personal Data

Ixion will ensure compliance with GDPR in respect of its storage of client/customer data. Therefore we assume that the key provisions of the DPA as set out below are being adhered by Ixion in its handling of client/customer data:

i) collected and used for specified purpose only;

ii) adequate, relevant and not excessive in relation to the designated purpose;

iii) accurate and, where necessary, kept up to date;

iv) not retained for longer than is necessary for the designated purpose;

v) processed in accordance with the DPA and GDPR; and

vi) adequately protected by appropriate technical and organisational measures.

Where Ixion holds personal information about a customer/client in connection with any complaint, (including where such information is held on email) then this information should be held in accordance with the DPA and GDPR.

Archiving in line with Retention Periods

Hard copy documents on site that are no longer actively being used, but which need to be retained, should be prepared for archiving by the information asset owner e.g. contract manager for client information, Head of Department for internal functions.

Approved archiving boxes should be used to store documents that must be sealed and labelled, with a clear destruction date indicated. Where there is insufficient documentation to fill a box the information asset owner should coordinate with other Contract Managers and Heads of Departments to ensure the archiving facility is fully utilised – all archiving boxes should be full before being sent for storage.

All details of archived documents must be logged by the Finance Manager in the archiving record log. This will show details of the documents stored in the box, the destruction date, the source office location, the contract name/number where appropriate, and the storage location.

In the case of client files the Contract Manager must ensure that the relevant client database is updated with details of the archive box number, to enable easy retrieval of the hard copy file should this be required for audit or other purposes.

As boxes become ready for archiving the Finance Manager will organise for boxes to be stored in the internal archive or for a secure archiving company to collect the sealed boxes.

Destruction & Disposal

Before destroying data or documents, the information asset owner should check that the content is in fact what it is labelled to be (to avoid inadvertent disposal of documents) and assess whether retention is required to fulfil statutory or contractual requirements, to evidence events in the case of dispute, or to meet another operational need.

Disposal will be completed via a range of processes appropriate to the document/record, including:

- Confidential waste collected by a designated secure licensed refuse collection service e.g. ShredIt
- Physical destruction on site (shredding)
- Secure deletion of computer files by the IT Department
- Migration to external organisation e.g. prime contractor

Under no circumstances should paper documents containing personal data or confidential information be disposed of in normal waste bins. Where documents are

migrated to a third party, the records should be listed and signed for by the recipient. Ixion will retain a copy of the receipt for at least 3 years.

Quarterly monitoring of the archiving record log will identify boxes within the archive facility that have reached their destruction date. In the case of externally stored material, the Finance Manager will arrange for the boxes to be securely disposed of by the archiving company, obtaining written confirmation of their destruction and updating the archiving record log accordingly. In the case of internally archived material, the Finance Manager will follow the disposal methods above. In both cases the archive record log will be updated to show the date and method of disposal, and the staff member who authorised disposal.

While staff may delete individual electronic files within their own personal domain folder, secure destruction of electronic records and documents is restricted to the IT Team only. Data will be effectively over-written and made unrecognisable as per the Information Assurance & Security Policy.

Responsibilities

All employees are responsible for:

- ensuring documentation and data retained by the Company is accurate
- ensuring documentation relating to individuals is limited to that required to fulfil our contractual, employer or operational requirements
- maintaining the security and integrity of data/documents in line with our Data Protection and Information Assurance & Security Policies
- ensuring that information is collected, recorded and used in accordance with the principles of the Data Protection Act and GDPR.

Managers are responsible for:

- ensuring that employees dealing with client or third party data are aware of their responsibilities
- ensuring information is archived using a secure archiving company when it is no longer actively required within our premises
- disposal of documents within their area of responsibility is carried out securely
- records of disposal are maintained

The Ixion Board is responsible for:

- ensuring there are processes in place so that Ixion is compliant with UK law and contractual requirements.
- Ensuring that processes are in place so that Ixion employees, agents and contractors are compliant with the law and contractual requirements.

Monitoring & Review

Shaw Trust Compliance team through audits at Ixion will review Information Security during contract audits.

The Head of Service – IT will review and monitor electronic data retention and storage facilities and ensure the necessary back up functionality and assurances are in place.