The Hub Educational Services CIC
Data protection policy in accordance with the EU General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018

Written by Vanessa Brooks

Date Written September 2024
Review Date September 2025

Policy brief & purpose

The goal of the data protection policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections, e.g. by the customer within the scope of commissioned processing. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) and Data protection Act (DPA) 2018 but also to provide proof of compliance. Our data protection officer or DPO is Vanessa Brooks and the policy abides by the following legislation:

- The Data Protection Act 2018 (DPA)
- The UK General Data Protection Regulation (UK GDPR)
- The Digital Economy Act (DEA)
- The Freedom of Information Act 2000 (FOI)
- The Environmental Information Regulations 2004
- The Human Rights Act 1998
- Commercial data contracts and the Statistics and Registration Services Act (the SRSA).

The Hub Educational Services CIC is an alternative provision, tuition and SEND support not for profit organisation. We take data protection very seriously and ask permission from our clients before sharing or using images or sensitive data. The only exclusion to this would be in the matter of child protection where a child would be put at risk or harm by sharing of information. We are registered with ICO and have a registration document to show our commitment to compliance.

Our **Company Data Protection Policy** refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality that all data is handled appropriately and that we are compliant with relevant laws surrounding data protection and GDPR.

The seven golden rules for sharing information

Privacy Statement

Our contact details

Name: The Hub Educational Services CIC
Address:148 Loughborough Road, Hathern, LE12 5JB
Phone Number:07595757197
E-mail:vanessa@thehub-cic.co.uk

What information we collect, use, and why We collect or use the following information for student education and welfare:

- Names and contact details for students/children
- Names and contact details for carers
- Gender
- Pronoun preferences
- Date of birth
- Dietary requirements (including vegetarian, vegan, gluten free and halal requirements)
- Payment details and financial information including transactions
- Special Educational Needs and Disabilities (SEND) or additional support information (includes reasonable adjustments and special educational needs and disabilities)
- Welfare information (includes family and home life circumstances and history)
- Details of any criminal convictions
- Photographs
- Biometric data for identification, access or payment purposes
- Attendance and reason for absence data
- Account access information
- Exam results and qualifications

• Progress reports
• Information relating to compliments and complaints
• Exclusion, suspension and behavioural information We also collect or use the following information for student education and welfare:
• Health information We collect or use the following information for disciplinary investigations or to prevent, detect, investigate or prosecute crimes:
• Names and contact details for students/children
• Names and contact details for carers
• Gender
• Special Educational Needs and Disabilities (SEND) information (includes reasonable adjustments and special educational needs and disabilities)
• Attendance and reason for absence data
• Witness statements and contact details
• Records and reports
• Video recordings of public areas (including entrances and outside spaces to which some or all members of the public have access)
• Video recordings of student access areas (including classrooms, corridors, canteens and outside spaces to which students have access) We collect or use the following personal information for dealing with queries, complaints or claims:
• Names and contact details
• Address
• Video recordings of public areas
• Dashcam footage - inside vehicle
• Witness statements and contact details
• Financial transaction information • Information relating to health and safety (including incident investigation details and reports and accident book records)
• Special Educational Needs and Disabilities (SEND) or additional support information (includes reasonable adjustments and special educational needs and disabilities) We collect or use the following information for information updates or marketing purposes:
• Names and contact details
• Marketing preferences
• Records of consent, where appropriate We collect or use the following information for archiving purposes:
• Names and contact details
• Addresses We collect or use the following information for recruitment purposes:
• Contact details (eg name, address, telephone number or personal email address)
• Date of birth
• National Insurance number
• Copies of passports or other photo ID
• Employment history (eg job application, employment references or secondary employment)
• Education history (eg qualifications)
• Right to work information
• Details of any criminal convictions (eg DBS, Access NI or Disclosure Scotland checks) We collect or use the following information to comply with legal requirements:
• Identification documents
• Health and safety information
• Criminal offence data (including Disclosure Barring Service (DBS), Access NI or Disclosure Scotland checks) Lawful bases and data protection rights Under UK data protection law, we must have a “lawful basis” for collecting and using your personal information. There is a list of possible lawful bases in the UK GDPR. You can find out more about lawful bases on the ICO’s website. Which lawful basis we rely on may affect your data protection rights

which are in brief set out below. You can find out more about your data protection rights and the exemptions which may apply on the ICO's website:
• Your right of access - You have the right to ask us for copies of your personal information. You can request other information such as details about where we get personal information from and who we share personal information with. There are some exemptions which means you may not receive all the information you ask for. You can read more about this right here.
• Your right to rectification - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete. You can read more about this right here.
• Your right to erasure - You have the right to ask us to delete your personal information. You can read more about this right here.
• Your right to restriction of processing - You have the right to ask us to limit how we can use your personal information. You can read more about this right here.
• Your right to object to processing - You have the right to object to the processing of your personal data. You can read more about this right here.
• Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you. You can read more about this right here.
• Your right to withdraw consent – When we use consent as our lawful basis you have the right to withdraw your consent at any time. You can read more about this right here. If you make a request, we must respond to you without undue delay and in any event within one month. To make a data protection rights request, please contact us using the contact details at the top of this privacy notice. Our lawful bases for the collection and use of your data Our lawful bases for collecting or using personal information for student education and welfare are:
• Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
• Contract - we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
• Legal obligation - we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability. Our lawful bases for collecting or using personal information for disciplinary investigations or to prevent, detect, investigate or prosecute crimes are:
• Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
• Contract - we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
• Legal obligation - we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability. Our lawful bases for collecting or using personal information for dealing with queries, complaints or claims are:
• Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
• Contract - we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
• Legal obligation - we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability. Our lawful bases for collecting or using personal information for information updates or marketing purposes are:
• Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time. Our lawful bases for collecting or using personal information for archiving purposes are:

• Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time. Our lawful bases for collecting or using personal information for recruitment purposes are: Our lawful bases for collecting or using personal information to comply with legal requirements are:
• Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
• Contract - we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
• Legal obligation - we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.
• Public task - we have to collect or use your information to carry out a task laid down in law, which the law intends to be performed by an organisation such as ours. All of your data protection rights may apply, except the right to erasure and the right to portability. Where we get personal information from • Directly from you
• Parents or carers
• Local authorities or local councils
• Social services
• Other education establishments
• Health care providers
• Professional consultants
• Government websites How long we keep information For up to 10 years depending on the information. A full schedule of timelines can be found in our data protection policy. Who we share information with Others we share personal information with
• Parents and carers
• Local authorities
• Social services
• Pupil Referral Units (PRU's) or Education Otherwise at School Centres (EOTAS)
• Specialist teachers such as peripatetic workers or speech and language therapists
• Examination boards and bodies
• Organisations we need to share information with for safeguarding reasons
• Emergency services
• Relevant regulatory authorities
• External auditors or inspectors
• Organisations we're legally obliged to share personal information with
• Publicly on our website, social media or other marketing and information media How to complain If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice. If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO. The ICO's address: Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Helpline number: 0303 123 1113 Website: https://www.ico.org.uk/make-a-complaint

The type of personal information we collect

We currently collect and process the following information:

- Personal identifiers, contacts and characteristics (for example, name and contact details)
- Customer financial information
- Student educational and progress data
- SEND information
- Parental contact details including email addresses
- Personal documentation of staff members

- Employee Data

The rights of an individual:

Under the Data Protection legislation, data subjects have the following rights with regards to their personal information:

- the right to be informed about the collection and the use of their personal data
- the right to access personal data and supplementary information
- the right to have inaccurate personal data rectified, or completed if it is incomplete
- the right to erasure (to be forgotten) in certain circumstances
- the right to restrict processing in certain circumstances
- the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- the right to object to processing in certain circumstances
- rights in relation to automated decision making and profiling
- the right to withdraw consent at any time (where relevant)
- the right to complain to the Information Commissioner

How we get the personal information and why we have it

Most of the personal information we process is provided to us directly by you for one of the following reasons:
- To support our work with children and young people
- To assist in claiming renumeration
- To ensure staff meet the qualifying criteria

We also receive personal information indirectly, from the following sources in the following scenarios:
- Schools and the local authority
- Parents
- Alternative provisions
- External specialists such as Educational Psychologists

We use the information that you have given us in order to:
- Devise a suitable package and offer for our learners
- Contact schools and organisations we work with
- Contact and communicate with third parties
- Share information with commissioners of our services

We may share this information with schools, parents, The Local Authority, Social services, police and other supporting services.
Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing this information are:
(a) Your consent. You are able to remove your consent at any time. You can do this by contacting Vanessa Brooks

(b) We have a contractual obligation.

(c) We have a legal obligation.

Scope

This policy refers to all parties (employees, job candidates, customers/clients, suppliers etc.) who provide any amount of information to us.

Who is covered under the Data Protection Policy?

Employees of our company must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

CCTV

Within all of our buildings, there is CCTV this will be switched on by the 11th January 2024 and will remain on at all times. This CCTV is stored on an external cloud based hard drive and has been put up with both staff and safety. It is our policy that if there is an incident that has to be reported, the external agencies will have the right to access this footage without seeking further parental request.

Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

Actions

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Access to Data Under data protection legislation: Parents and learners have the right to request access to the information that we hold about them. Should staff be approached with such as request, please direct them to the DPO or to contact us directly through our website. SARS requests usually take no more than 28 days and a written copy would cost £10. If a child is under 16 then this request would usually be made through a parent or carer. Children over the age of 14 may make the request alongside parents.

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

Data Retention length

Employee Data (Permanent & Fixed Term)

Activity/Information	Description	Start of Retention	Retention Period
Unsuccessful Recruitment Candidates	Personal Information	Last action on the applicant file	2 Years
	Application Forms & Supporting Documentation	Last action on the applicant file	2 Years
	Recruitment Vetting & Criminal Convictions	Last action on the applicant file	12 Months
	Identification Documents	Last action on the applicant file	3 Months
Successful Recruitment Candidates	Personal Information	Last action on the applicant file	6 Years
	Application Forms & Supporting Documentation	Last action on the applicant file	2 Years
	Recruitment Vetting & Criminal Convictions	End of Employment	6 Years
	Identification Documents (including Identification Documents of Foreign Nationals (ensuing from obligations to retain copies of documents used to perform immigration checks)).	End of Employment	6 Years
Employee Records	Employee Personal Details	End of Employment	6 Years

Activity/Information	Description	Start of Retention	Retention Period
	3rd Party Emergency Contact Details provided by employee	End of Employment	6 Years
	Bank Account Details	End of Employment	6 Years
	Additional Personal Details (e.g., Religion, Ethnicity, Disabilities, Gender Identity)	End of Employment	6 Years
Employment File	Written Particulars of Employment	End of Employment	6 Years
	Personal Payroll History/Salary records (including record of pay, performance pay, overtime pay, allowances, pay enhancements, other taxable allowances, payment for untaken leave, reduced pay, maternity leave)	The end of the assessment tax/period to which the payments relate	6 Years
	Pensions Records	Date of Birth	100 Years
	Expenses Records	The end of the assessment tax/period to which the payments relate	6 Years
	Appraisals/Assessments	End of Employment	6 Years
	Annual Leave Records	End of Employment	6 Years
	Unpaid Leave Periods (Records of Maternity, Paternity, Adoption or Sick Leave)	Date of Birth	100 Years
	Statutory Maternity Pay Document	The end of the tax year in which the maternity pay period ends	6 Years

Activity/Information	Description	Start of Retention	Retention Period
	Complete Sickness Absences Record showing dates and causes of sick leave	End of Employment	6 Years
	Medical/Self Certificates	End of Employment	6 Years
	Health Referrals (including medical reports from doctors/consultants)	End of Employment	6 Years
	Health & Safety Records	The end of financial year to which the records relate	6 Years
	Death Benefit Nomination & Revocation Forms	From Leaving Employment	6 Years
	Staff Security Vetting Records	From Leaving Employment	6 Years
	Employee Training Records	From Leaving Employment	6 Years
	Employee Grievance Records	From Leaving Employment	6 Years
	Working Time Records	The end of the financial year to which the records relate	6 Years
	Employee Discipline Records	From Leaving Employment	6 Years
	Job History	From Leaving Employment	6 Years
	Redeployment, Redundancy & TUPE	From Leaving Employment	6 Years
Contingent Workers	Contingent Worker Record (name, address, contact details)	End of Employment	6 Years
Operational Records	HR Operational Records	Last Modified Date	2 Years

Customer Data

Activity/Information	Description	Retention Period
Applications (Where applications are abandoned, or no funding is provided)	• Applicant Record • Customer Funding & Previous Study Record • Customer Application • Health Information • Eligibility/Entitlement • Customer Account, Engagement & Supporting Information • Customer Information Provided to/from 3rd Parties • Parent/Guardian/Partner/Associated Party Information & Supporting Documentation for Applicants • Operational Artefacts • Voluntary Statistical Data • Payment & Fraud Investigations	Certain customer data is currently retained on an indefinite basis within SLC. SLC has other obligations to ensure that customer data is retained in line with a range of regulatory and business requirements. In certain circumstances SLC is required to keep data for a minimum length of time (e.g., financial information) and/or even the lifetime of the customer. For example: • student support legislation obliges SLC to take into account any previous supported study to accurately determine an individual's entitlement to student support for any further study; and • student finance eligibility criteria requires that there are no arrears with any previous student loans.
Customer Record – Repayable Funding	• Core Customer Record • Customer Funding & Previous Study Record • Customer Application Record(s) • Health Information • Eligibility/Entitlement Assessment • Customer Account, Engagement & Supporting Information • Customer Information Provided to/from 3rd Parties	As above

Activity/Information	Description	Retention Period
	• Operational Artefacts • Voluntary Statistical Data • Payment & Fraud Investigations	
Correspondence	• Customer Specific External Correspondence (Apply to Pay Phase of Customer Lifecycle) • Customer Specific External Correspondence (Repay Phase of Customer Lifecycle) • Customer Specific Internal Correspondence (Apply to Pay Phase of Customer Lifecycle) • Customer Specific Internal Correspondence (Repay Phase of Customer Lifecycle)	As above
Parent/Guardian/Partner/Associated Party/Additional Contacts Information	• Parent/Guardian/Partner (Sponsor) Core Record • Parent/Guardian/Partner (Sponsor) Financial Information • Parent/Guardian/Partner (Sponsor) Dependents • Parent/Guardian/Partner (Sponsor) Declaration • Consent to Share • Power of Attorney • Additional Contacts • Operational Artefacts	As above
Appeals	• Appeals Case Files • Operational Artefacts	As above

Activity/Information	Description	Retention Period
Customer Complaints, Research & Feedback	• Complaints & Feedback Case Files • Operational Artefacts • Customer Research (Customer Specific) • Customer Research (Unattributable/Anonymous) • Operational Artefacts	As above
Counter Fraud	• Counter Fraud Case Files • Operational Artefacts	As above

Corporate Management and Governance

Activity/Information	Description	Start of Retention	Retention Period
Statutory Books, Registers and Constitutional Records	• Incorporation documents • Companies House Correspondence • Companies House Filings • Company Books and Registers	Date of most recent document	Permanent (Life of Company)
	Gifts and Hospitality Register	End of Financial Year	10 Years
SLC Board	Board Effectiveness – various working papers	Date of most recent document	10 Years
	Board Schedule	Date of most recent document	5 Years
	Board Minutes of Meetings	Date of last action	Permanent
	Board Reporting Protocols	Date of most recent document	5 Years

Activity/Information	Description	Start of Retention	Retention Period
Board Member Information	Board Member Details including: • Letters of appointment and delegations • Contact Details • Letters of Indemnity • Register of Interests • Induction Paperwork • Various files & advice • Skills & Assessment	After end of appointment/employment	5 Years 6 Years
Operational and Business Administration	• Policies and Procedures • Policy Specifications	When updated/superseded	Superseded Permanent
	Operational Business Information (General administrative records, routine administrative correspondence (not related to customer, contract or legal matters)	Date of most recent document	2 Years
	All other Corporate Management and Governance Records	Date of most recent document or last action in most cases	6 Years in most cases. . Some records, e.g., Letters of Financial Delegated Authority, Annual Performance and Resource Agreement, Framework Documents and External Reports are kept permanently.
Planning and Performance	• Corporate and Business Plans • Annual Report and Accounts • Performance Reports • Management Information	Financial Year End	7 Years
Audit	Audit Reports and Report Papers	From issue date	6 Years

Activity/Information	Description	Start of Retention	Retention Period
	Interim Audit Reports, Correspondence and Internal Audit Guides	From issue /correspondence date	3 Years
Projects	• General projects • Financial documents • Policy project documentation • Initiation documents • Project proposals • Plans and specifications • Draft reports and working papers • All related project correspondence	Completion of Project / date of last paper	6 Years Major projects determined by their nature can be retained for longer up to 25 years
Legal Affairs	Provision of legal advice not specific to an individual case (etc. Legal advice given to SLC concerning legislation or proposals for new legislation affecting its conduct and business) Includes legal advice for projects, contracts, policy and in relation to a dispute.	Date of advice	7 Years
Procurements and Contracts	Tenders, Contracts and Agreements	End of Contract	6 Years
	Settlement Agreements with ex-employees	Date of Agreement	6 Years
	Non-Disclosure Agreements	Date Non-Disclosure Agreement ceases to have effect (NB – may be indefinite)	6 Years
Litigation	• Employment Tribunal Records • Civil Court Litigation	Date file closed (which will not be earlier than appeal deadline)	6 Years

Activity/Information	Description	Start of Retention	Retention Period
Intellectual Property	Branding and intellectual property (including trade/service marks)	Date modified	Life of Company
Commercial Property	All documents relating to SLC's property portfolio	Date deed is superseded in full or terminated	6 Years
	Land and Buildings Transaction Tax (LBTT) Returns to Revenue Scotland	Date relevant lease ceases to apply	6 Years
Access to Information (Information about Freedom of Information, Data Subject Access Requests and the Publication Scheme)	Procedures for handling FOI requests and other documents regarding implementation of FOI; Procedure and Policy, case file records which lead to the development or precedent or best practice	When updated or superseded	6 Years
	Case file records detailing FOI requests and responses, consideration of exemptions, and subject internal reviews and appeals. Each case record is likely to contain personal data as defined in UK data protection legislation. Specifically, each record is likely to contain: • the name, address, and other contact information of the applicant • personal details provided by the applicant when making his/her request • where a fee has been paid, bank account and other payment details • all personal data will be handled with care and in accordance with UK data protection	From date of release	6 Years

Activity/Information	Description	Start of Retention	Retention Period
	legislation. Access to personal data will be strictly controlled.		
	Data Protection "Rights of Data Subject" records – to include Subject Access and Data Portability requests, requests for erasure, rectification, restriction, objection. Includes initial request, response, related correspondence and other supporting documentation	Completion of Request	6 Years
	Statistical data about number of FOI requests and Data Subject Access requests. Includes the timeliness of responses, outcomes, internal reviews and appeals and management information	Current Year	10 Years
	Details of what access decisions have been taken about SLC records and redacted versions of documents that were released	Current Year	10 Years
	Information subject to a FOI request but scheduled for destruction	Last date of correspondence	6 Months
	Publication Scheme published on the SLC website	When updated/superseded	5 Years
Risk Management	• Audit Risk Committee Risk Report and Dashboard.	Date superseded	5 Years

Activity/Information	Description	Start of Retention	Retention Period
	• Database containing all of SLCs historic and current Corporate Risks and issues	End Date	6 Years
Business Continuity	• Business Impact Analysis • Business Continuity Plans • Post-exercise / post incident reports • Supplier review	At the start of each year	5 Years
Print and Mail Services	• Memorandum of Understandings • Service Level Agreements • Licence Agreements	At the start of each agreement and refreshed annually	Permanent
Health and Safety	Risk Assessment documents for all sites listing hazards or hazardous events and the actions and controls in place to manage these	Updated annually or if/when a change is required	6 Years
	Health & Safety Committee Meeting Minutes	Quarterly when document created	5 Years
Partner Services and External Engagement	Includes documentation but not limited to minutes of meetings, agendas, presentations, data capture forms, satisfaction surveys, all communications, performance review reports, analytical data, service agreements and contracts, audit reports, guidance, factsheets, web service/online content.	Creation of document / when updated or superseded	When no longer required / Superseded
Public Relations and Press	Press Cuttings and Press Releases	From publish date	2 Years
	Emails with journalists to inform reporting of media stories	From release date	2 Years then Archived

Activity/Information	Description	Start of Retention	Retention Period
	Correspondence with the media	From date of correspondence	Permanent
	Information and guides	When updated/superseded	Superseded
Internal Communications	Staff communications	When administrative use ends	3 Years
	Intranet pages	From publish date	When no longer required
Images, Templates and Corporate Identify	Images of various SLC offices, staff and events	From publish date	When no longer required
	Corporate identity material, logos and stationery	When updated/superseded	Superseded
Online Content	All Web Content	When updated or superseded	Superseded
	Social Media including messaging that goes out through various communication channels, links to websites	From publish date	Superseded
	Campaigns and Materials including web adverts and emails	Conclusion of campaign	3 Years
	Plans for Delivery (including web content and delivery)	When updated or superseded	Superseded
	Guides and Facts Sheets – for all domiciles downloadable from web channels	When updated or superseded	Superseded
	Films – animated explainers, piece to camera of colleagues	From publish date	Permanent

Activity/Information	Description	Start of Retention	Retention Period
Publications, Presentations and Correspondence	Guides distributed domiciles e.g., Universities	When updated or superseded	Superseded
	Presentations for practitioners to teach students about Student Finance	When updated or superseded	Superseded
	System generated letters and emails sent to customers	When updated or superseded	Superseded
Marketing Analysis	Information identifying customer needs and all other marketing materials for analysis	When updated or superseded	Superseded
Governance and Compliance (SLC Compliance Framework, Security Assurance Management, Data Protection Management, Records Management, Data Governance and Knowledge Management)	Reference Materials	Current Year	2 Years
	General Compliance Artefacts	When updated or superseded	6 Years
	Populated Artefacts and Compliance Records: Documents and correspondence related to the application of the Control Compliance Framework, Security Project Delivery Model, Data Protection Principles and GDPR, Records Management Framework, Data Governance and Information Asset Owner Framework.	From start of control framework or Current Year	From 6 Years to Lifetime of System/Process
	Mandatory Artefacts: • Privacy Notices • Notification to the ICO • Records Retention Schedules • Related Risk Registers • Information Asset Registers	When updated or superseded / Current Year	From 6 Years to Permanent
	Statistical Data and Reporting including Management Information packs and dashboards	Current Year	6 Years

Activity/Information	Description	Start of Retention	Retention Period
	Data Protection Case File Management	Closure/Date of Last Action	6 Years (cases of interest may be retained for a further 2 years, on a 2 year review rolling basis)
Independent Assessor (IA)	Reports, Case File, Evidence	Date IA report issued	10 Years
	Ombudsman Reports	Date IA assigned to role	6 Years
	Customer Recordings	End of Period of Study/Closure of Case	6 Years
	Annual Reports	Date of report	6 Years
	Contact Information	Date of IA assigned to role	11 Years

Financial Management

Activity/Information	Description	Start of Retention	Retention Period
Accounting Records	• Bank Account Records • Financial Statements and Summaries • Management and Project Account Forecast Reports	End of the financial year to which the records relate.	6 + 1 Year
Transaction Records	• Record of cheques drawn for payment • General and subsidiary ledgers Financial transactions • Operational Records • Money Laundering Reporting Officer (MRLO) forms and Investigation log	End of the financial year to which the records relate. When referred to MLRO	6 + 1 Year 2 Years 5 Years

Activity/Information	Description	Start of Retention	Retention Period
	• Sanction Records	When added to Sanctions List	Indefinite – until removed from Sanctions List
Employee Financial Records	• Payroll Records	End of the financial year to which the records relate	6 + 1 Year
Assets and Equipment	Assets and Equipment Registers	End of the financial year to which the records relate	6 + 1 Year
Procurement	• Contracts • Tenders • Purchase Orders	Expiration of contract in most cases	6 + 1 Year

Information Communication and Technology

Activity/Information	Description	Start of Retention	Retention Period
Information Security Management	• Incident Management Register • Incident Management Case Records • Incident Management Data Breach Detection Records	• Last Action on File • From Closure of Case • Last Action on File	6 Years
	• Management information • Service level data sheets • Data Security Team operational reports, • Issues, monthly trend and common trends	When updated/superseded	3 Years
	Data Security Work Instructions	When updated/superseded	4 Years
	Data Transfer Authorisations	Last modified date	6 Years

Activity/Information	Description	Start of Retention	Retention Period
	Third Party Reviews	Last modified date	6 Years
	Network and system access logs	Date of access	Up to 3 Years
Technology Change and Integration	Artefacts created and retained for project delivery and in conjunction with business services alongside project lifecycle	Date of issue or completion of project	6 Years
Architecture	• Architectural Design Papers • Architectural Level Papers	When updated or superseded	Indefinitely
Technology Operations	• Compliance Tracker Documents • Performance Initiative Documents • Executive Reports • Service Review Packs • Planning Materials • Policy and Process Documentation • Process Trackers	When updated or superseded	Indefinitely
	• Demand and Capacity Reporting • Technology Group Spot Awards	End of Year	6 Years
System User Training and Support	• Learning/Training Packs and Documentation including supporting documentation • Process Maps	When updated or superseded	2 Years

Data Breaches

A data breach is any instance where personal data is accidentally or unlawfully disclosed, destroyed, lost or altered or if there is unauthorised access to personal data, either in hard copy or electronic, including through cyber-attacks.

+Any breach or suspected breach must be reported immediately to the DPO, who will take further action as described below:

1) Review the circumstances and nature of the breach and, where needed alert an NLT director to assist in ongoing investigation, containment, reporting to police and follow up actions.

2) Take steps to halt the breach (if still ongoing), and to minimise reach and impact of the breach, including notifying the bank of any financial risks, and pausing access to email accounts, changing any access codes or passwords as needed.

3) Inform the Information Commissioner's Office (ICO) within 72 hours including any known or risk of impact on individuals, communities or groups – eg if released emails may become involved in phishing attacks.

4) Agree a Plan of communications to individuals who may be initially affected

5) A full investigation will then be undertaken, with follow up communications to all involved in the steps taken to rectify and reduce further risks.

Further reading:

- Data Protection Act of 1998 (UK)