The Learning Support Centre
Dyslexia & Disability Specialists

Policy	Data Protection and Data Sharing Policy Procedures
Issue date	03/2012
Author	Laura Cook, Managing Director
Approved by	Donna Welburn
Last review	08/2023
Review date (m/y)	08/2024

Scope of Policy

To carry out its statutory and administrative functions The Learning Support Centre (LSC) collect, hold and process personal information relating to many categories of people (data subjects) including clients, employees, applicants to work and suppliers. We recognise the right to confidentiality and security of personal information and therefore take all reasonable steps to comply with the principles of the Data Protection Act 1998, General Data Protection Regulation (GDPR) 2018 and Human Rights Act 1998 (article 8)

This policy applies to all employees, subcontractors, and volunteers of LSC. This policy and procedure set out guidelines about how we handle data and the information that should remain confidential and who may need to know certainpieces of information and under what circumstances:

- This policy applies to all personal data held by LSC irrespective of whether it is held on manual or electronic media.
- LSC will only process and hold personal data for those purposes notified to the Information Commissioner.
- LSC will only hold data if we have a legal basis to hold it.
- LSC will not disclose personal data to any third party without written consent from the data subject, save where required by law or statutory obligations.
- Personal data is not kept longer than necessary.
- LSC seek to provide a high standard of security for all personal data whether it is stored on computer, cloud or in alternative filing systems.
- LSC treats all information about its data subjects as confidential and all employees and contractors working with clients are required to sign a confidentiality agreement prior to commencing work.

Requirements for Implementation

LSC will perform an annual data audit of all non-automated filing and information systems.
This audit will enable the company to maintain an inventory of data systems in use within the organisation and ensure data is accurate and up to date.

In deciding if a data store is relevant, filing system criterion will be applied, namely:

- Information is grouped by theme.
- Information is structured by reference to name, number or other mechanism such as type of job or section.
- Information is structured to enable easy access to information about individuals by authorised personnel only.

Training

All LSC employees are asked to carry out GDPR Training. The management team is committed to this policy and proactive in ensuring it is adhered to therefore GDPR and cyber security is covered in induction training and annually with all LSC employees.

Processing data

The LSC receive data from third parties and data subjects directly, at which point we establish a lawful basis and request explicit consent from the data subject. To remain transparent, we refer clients where we hold personal data to our privacy notice which can be found on the LSC website. If we want to process the data for additional purposes, we send an additional request for permission.

Access to data

Access to personal data is on a need-to-know basis and unlawful access to and/or disclosure of personal data is prohibited. Office-based employees have data access rights determined by their job description. All IT equipment and software is password protected with unique, individual passwords; users are prompted to change passwords every 90 days and have MFA (Multi Factor Authentication) set up on their accounts.

Data storage and disposal

All manual data must be stored in locked cabinets and not left on unoccupied desks. Electronic data is stored on a password protected database and is only accessible to authorised users. Manual data must be shredded and dealt with as confidential waste. Electronic data will be deleted permanently or archived in line with the above.

Subcontractors

All subcontractors sign a data sharing agreement and consent to share is sought by the data subject. Transfer of data is done via password protected database or files.

Policy	Data Protection and Data Sharing Policy Procedures
Issue date	03/2012
Author	Laura Cook, Managing Director
Approved by	Donna Welburn
Last review	08/2023
Review date (m/y)	08/2024

Dealing with a data breach

It is important all actual or suspected data breaches should be reported. Please notify Donna Welburn, Data Protection Officer immediately. Immediate responses are required so the impact of any data breach can be mitigated.

Sharing data

Employees will not disclose information about a client to people who do not need to know it. Sometimes situations may arise where it would be appropriate to break confidentiality or divulge information. Circumstances which may be considered as appropriate are as follows:

- Where it is considered by the employee in receipt of the information that an individual will be placed at risk of physical danger and withholding information could cause harm or injury to an individual.Where it is disclosed or considered that a criminal offence has been or will be committed.
- When information is disclosed about acts of terrorism.
- The disclosure of information relating to the protection of children.
- The disclosure of information relating to the protection of adults at risk as defined by the Care Act 2014.

Where it is considered essential to break confidentiality, the person whose confidentiality is to be broken, in normal circumstances, is informed.
Any threat of self-harm, violence in relation to an employee or client, or a serious threat against another person will be recorded and reported to the employee's line manager. LSC have a duty of care under health and safety legislation to employees, clients and those associated with LSC.

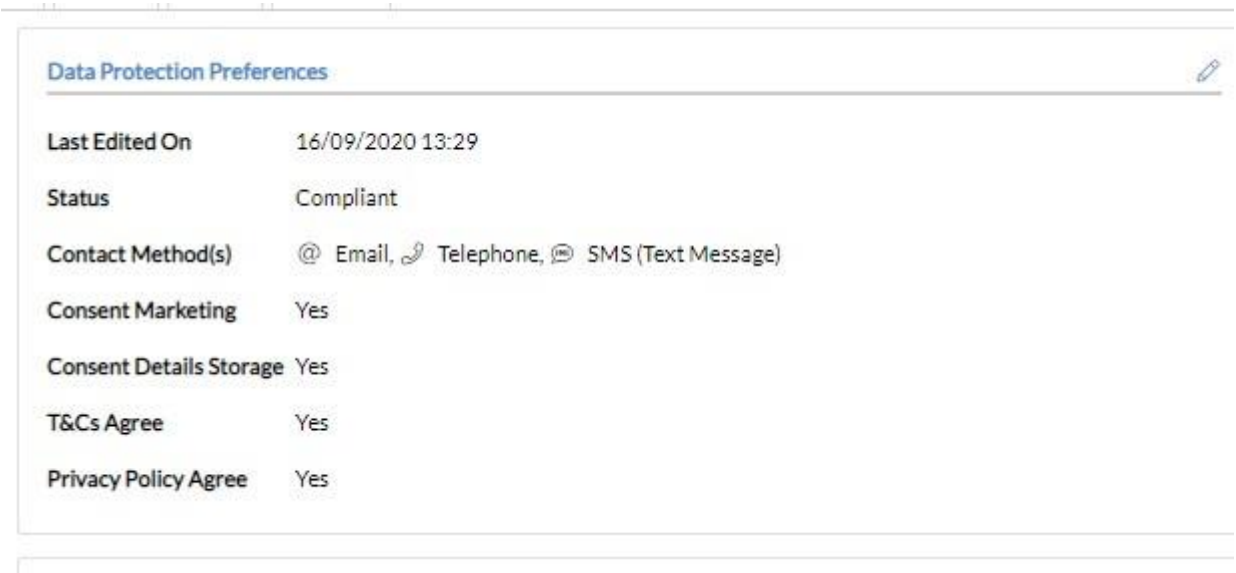
Action by line management when assessing whether to disclose confidential information to external agencies without the consent of a client

If the line manager believes that confidential information should be passed onto another party or agency, without the client's consent, they should brief the Operations Director, or in absence, the Managing Director on the full facts of the case. If the Operations Director agrees that action is required, a full report onthe case will be made and any agreed action undertaken. The line manager is responsible for ensuring that all necessary actions are taken.

The procedure to be followed when a break of confidentiality needs to be made is as follows:

- The support employee involved will raise the issue with the supervisor or line manager to discuss
- why confidentiality should be broken.
- A discussion regarding what the action will achieve.
- An agreement on a course of action and which external agencies might be contacted for example police, social services, GP, emergency services, university or college disability advice service, and faculty disability coordinators.

Where we hold personal information on clients, we will have a password protected account for them via our CRM system. When they log in for the first time their data protection preferences will be asked, and they can amend these at any point.



Subject Access Requests (SAR)

A subject access request is a written or verbal request made by or on behalf of an individual for the information held on them, thus:

- Requests should be referred to the Data Protection Officer Donna Welburn.
- The identity of the individual making the request will be sought.
- LSC will ask the subject for additional parameters or the specific pieces of information that individuals need from the SAR.
- There are some exemptions, which means you, the subject may not always receive all the information

LSC process. If the LSC consider a request to be manifestly unfounded or excessive then you, the subject will be charged an admin fee.

- Information should be provided without delay and within 30 days of the request.
- Due to the databases used by the LSC, the subject may be offered a time when they can come in to view their records on the system depending on the extent of their request.

Clients and Confidentiality and Information Sharing Procedures

Decisions about who has information will be made through the line management structure. This

emphasises that sharing information with your line manager will not be seen as a breach of confidentiality.
A record will be kept of all meetings and decisions, either as minutes or file notes. This should include anote of who that information has been shared with including clients, families, carers, advocates,professional workers etc.

Employee Confidentiality and Information Sharing Procedures

Personnel files can be accessed via PeopleHR by the employee's direct line manager, supervisors and as required by the senior management team, finance officer for payroll purposes, HR and support administrator tosupport keeping accurate records for LSC.

Employees can have access to their own file, including references and third-party information, having given notice.

Sensitive information held for equal opportunities monitoring purposes may only be accessed by authorised employees.

Supervision Files will be:

- Held by the employee's direct line manager and are stored on PeopleHR.
- Contain supervision notes, notes pertaining to informal discussions between the employee and their manager/supervisor and notes of any discussions pertaining to monitoring of performance e.g. appraisaldocumentation.
- They may also contain records of annual leave/other absences.
- The supervision files can be accessed through the line management structure. Managers above the direct line manager can also access supervision files.

Specific Instances of Information Confidential to Employees

There are several situations where it is a specific responsibility of the line manager to ensure thatthey do not release the nature of information concerning an employee.

Sickness

Employees that are sick should give information about the nature of their sickness to their line managerand should submit any sickness certificate to them. This information will also be passed to the OperationsDirector and payroll. Reasons for employee's absence due to sickness should not be discussed outside ofthe line management structure. Other than this, the individual will decide who else should know what about their state of health and pass the information on accordingly.

Other Special Leave

In order to take a view on the appropriateness of a request for leave the line manager will need to know why it is required. A note of this should be made in the employee's supervision file. The nature of the special leave may be relayed to others, but not the reason.

Recruitment

Who applies for posts, whether they are short listed, whether they are appointable, is all confidential information, until the person has accepted the job offer. It can be very uncomfortable for internal candidates when their colleagues have this information. People involved in the recruitment process should be particularly mindful of the confidentiality of internal candidates.

Disciplinary and Grievance

Any information within LSC, whatever its status, may be used for the purposes of investigating and resolving a disciplinary or grievance matter and must be relayed by employees with knowledge of the matter under investigation. Please refer to the LSC policy on discipline and grievance for furtherinformation.

There is potential for a great many people to become aware of some pieces of information as any investigation proceeds. It is important for both the investigator and the complainant/appellant to remember that neither is empowered to discuss the situation with others outside of the following: any union or other formal representative; individuals who may be substantive witnesses about **relevant** information to their involvement; managers who may be assisting with the investigation.

Any written documentation pertaining to the investigation or grievance might also be seen by the administrator.

If a disciplinary penalty is awarded, this will be placed in the employee's personnel file. Copies of

correspondence pertaining to any formal grievance will also be placed on the employee's personnel file.

Media

From time-to-time LSC may be asked for information about the service and the functioning of the organisation itself for media purposes.

All requests for information for the media relating to clients or employees must be agreed by the operations director or managing director.

In all cases a written agreement should be made covering what information is required, for what purposes and how it is to be presented. The client or employee should sign this in agreement before any information is used for media/marketing purposes.

Phone Call and Other Conversations

All employees must be vigilant around the making and taking of phone calls particularly in shared offices and in public places when using a mobile phone. Where you think other people may overhear a confidential conversation, you should relocate the call to a more private space.

Clear Desk / Clear Wall Issues

Confidential information should not be left visible and unattended on desks or in filing trays where there is easy access. It should never be posted on walls. Where information is unattended temporarily it should be removed by being put in an envelope or drawer, given to someone for temporary safekeeping or the office should be locked.

Important Guidance for Support Employees Working Off Site

'Sensitive' personal data has to be handled with special care and we normally need to have the person's explicit consent for the use of this information unless it is related to a safeguarding issue. Please refer to the **Safeguarding Policy and Procedure.** Sensitive personal date includes political opinions; religious beliefs or beliefs of a similar nature; sexual health; criminal records; ethnic background; physical or mental health conditions; commission or alleged commission of an offence; and any court proceedings relating to the commission or alleged commission of an offence.

Keep personal data secure at all times; this is particularly relevant to your role as you may be travelling with client's personal data.

- Ensure client information is not left in your car overnight.

- Do not travel with client information unless necessary.
- Return all client information to the office once support has ceased.
- Ensure that once client's information is no longer required, it is returned to the office for confidential shredding.
- Ensure that you are aware of when you can and cannot share personal data;
- Do not sharing client's personal data and information outside of the office, this includes with colleagues if they are not involved in supporting the client.
- Ensure discussions regarding clients only take place with your line managers and seniors in a confidential environment.
- Ensure that discussion of shared clients takes place in a confidential setting.
  Ensure you have secure passwords for Cobalt and your caseload spreadsheet.
-

The office will deal with requests from the police for personal data. Unless it is a genuine emergency, the

request should be made in writing on the polices own form and disclosure should always be authorised by the Operations Director or Managing Director.

If we are to share client or employee information with partner organisations this needs to be agreed with the individual. This is why the Service Agreements and Consent to Share request in the client's welcome email are essential.

Do not keep personal data for longer than necessary, we must have a good reason for keeping personal information and should not store it for longer than necessary. Ensure you give any client information back to the office when it is no longer needed so it can be recorded centrally or destroyed.

Ensure you know how to recognise a subject access request (SAR). A subject access request is a request by someone for a copy of their own personal information (e.g., a request for 'a copy of my client/employee file', 'any information you hold on me', or 'all information relating to my complaint'). Please contact your line manager if you receive this kind of request.

Be aware that anything you write down about someone could be disclosed to them, subject access requests can include the disclosure of e-mails and handwritten notes to the individual as well as more formal documents.

Personal data also includes information which can indirectly identify someone, for example, if you have a list of clients in a group which states that one person uses a wheelchair, this could be enough information to identify that person even if you don't have their name on the list. Essentially if someone can be identified from the information, it is classed as personal data.

Policy	Data Protection and Data Sharing Policy Procedures
Issue date	03/2012
Author	Laura Cook, Managing Director
Approved by	Donna Welburn
Last review	08/2023
Review date (m/y)	08/2024

Named Data Protection Officer: Donna Welburn

Related Policy and Supporting Documents

The Data Protection Act
Guide to the General Data Protection Regulation (GDPR)
The Human Rights Act 1998 (article 8)
Safeguarding Policy and Procedure
LSC Privacy Notice
HR Data Processing Impact Assessment
Client Data Processing Impact Assessment
PeopleHR Terms and Conditions
Cobalt Term and Conditions
Cyber Safety Policy
Staff Portal – Data Protection and Cyber Security Guidance