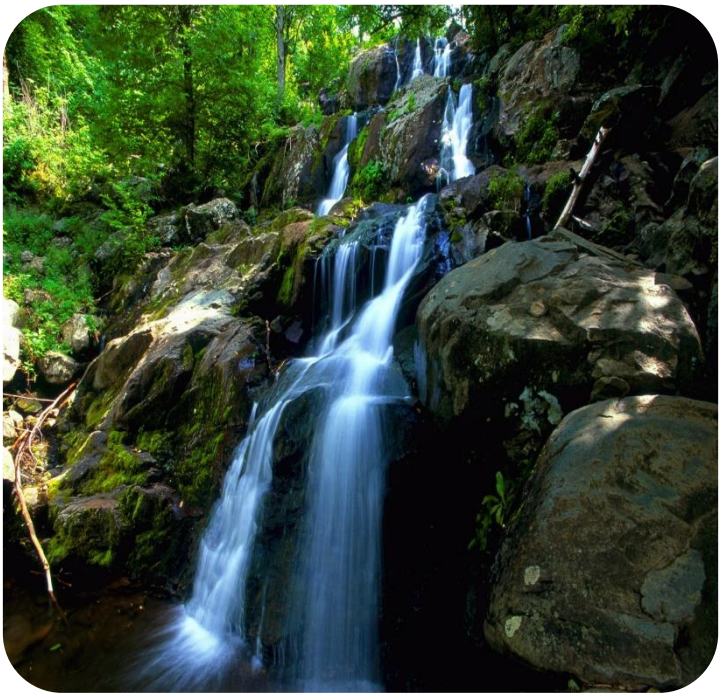
Lewis & Graves Partnership

Privacy Policy



L&G FACILITIES MANAGEMENT SERVICES	Privacy Policy

IMS Number	Document Number	Person Responsible
IMS68	CP - 02	General Manager

Aims

The main aims of this policy are to:

- Ensure that the organisation complies with the GDPR and the associated Codes of Practice.
- Ensure that information given in trust by users of the organisation services and staff members or held within the organisation for any other reason is treated with respect.
- Ensure that information is protected through clarity about how it is to be stored and shared.
- Ensure that the boundaries of confidentiality are clear and understood by staff.

The Policy is designed to:

- Ensure the organisation complies with GDPR and Associated Codes of Practice.
- Protect the best interests of staff and service users
- Make explicit the responsibilities of staff concerning confidentiality and privacy.
- Ensure users are aware of the organisation's responsibilities to protect confidential and private information.

Principles

This policy covers confidential and private information relating to staff and service users of the organisation. It is based on the principal that all such information should be treated as confidential. Information of this nature should only be shared when there is a clear, legitimate reason for doing so and with the permission of the staff member of service user concerned.

Although personal/sensitive information is protected by the organisation there are exceptional circumstances when confidential information would have to be disclosed. (These circumstances are noted in section 11 of the policy.)

Storage and Disposal of Information

It is the responsibility of the organisation's staff to ensure that personal/sensitive information about service users (individual clients, members, groups and organisations) is treated as confidential and stored in a secure place.

Such information will be stored only if it is current and necessary to undertake tasks relating to service delivery.

The time limit for storage of general non-active information will be 5 years, where this is a legal requirement to do so. Information where there is no such legal requirement will be stored for an appropriate period of time, which may, on occasion, be specified. There may be instances in which information of a personal nature is held longer than 5 years at Management's discretion.

The organisation's staff will be responsible for shredding confidential papers when finished with and deleting them from computer files.

L&G FACILITIES MANAGEMENT SERVICES	Privacy Policy

Access to Information

The organisation is on the Data Protection Register and adheres to principles and practices outlined in the Data Protection Act 1998.

The organisation operates an Open Access Policy in relation to files and computer records, whereby service users and staff members have access to information held about them. In order to access information, service users would be obliged to give the Chief Executive of the organisation two working days' notice.

Information regarding service users is confidential to the team from whom they receive a service, and not to the individual staff member working with them.

Information considered sensitive regarding an individual service user and affecting the work we are engaged in with the user should be reported to the employee's line manager, who is responsible for monitoring the situation outlined.

Only information regarding users which is directly relevant to service provision will be held on record. Information given for one purpose will not be used for another purpose.

In the case of working with a group, individual group members have the right to access general group files stored at the organisation but not to personal information about other group members. Likewise, personal information e.g. phone numbers, addresses, relating to staff members will not be given to other staff members or service users without the permission of that person.

Boundaries of Confidentiality in Supervision Within the Organisation

In supervision, confidential information can be discussed relating to professional and, at times, personal issues when they are affecting the individual staff member's work. The supervisor is responsible for treating this information as confidential.

The supervisor has the responsibility to ensure that recordings of supervision sessions are kept in a secure place.

All information discussed in supervision will be considered confidential by both the Supervisor and the staff member being supervised.

Some issues arising in supervision may need to be discussed with the Chief Executive in order to reach a resolution. In this situation, both the supervisor and staff member being supervised should agree to this course of action.

In the event of issues arising, within a supervision context, which require to be dealt with in a line management capacity, e.g. disciplinary issues, the supervisor will call a separate line management meeting, and the Chief Executive will be informed about this action.

Personnel Files

Personnel files are confidential, with access to a staff member's file being limited to the Human Resources Manager and to the individual at any time during office hours. Personnel files are kept up to date by the Human Resources manager who, can access these files for this purpose only.

Personnel files will be kept in a locked filing cabinet, with the Human Resources manager holding the keys.

L&G FACILITIES MANAGEMENT SERVICES	Privacy Policy

Personal Issues Affecting Staff Members

Staff members have the option of discussing personal issues adversely affecting their work in confidence with their line manager and the Human Resources manager and they can then take appropriate measures to address these issues without breaking confidentiality subject to the staff member's agreement. This may include discussion with an appropriate other person and placing a record of this into the staff member's personnel file.

When sickness leave is taken a sickness, line must be sent to the line manager / Human Resources manager. Information on the nature of the illness will not be made known to other staff members. To ensure this, sickness lines should be submitted in sealed envelopes and marked confidential.

Telephone Calls and Letters

Any mail sent to a staff member and marked Private and/or Confidential will not be opened by another staff member.

Access to a room where phone calls can be made in private will be available to staff working in open plan offices.

Breaking Confidentiality

Staff are required to maintain confidentiality in accordance with this policy. Inappropriate disclosures will be treated as a disciplinary matter and dealt with in accordance with disciplinary procedures. Action taken may include dismissal.

Exceptional Disclosure of Information

Exceptional circumstances may occur where the protection of a service user, a staff member or a third party or another person must be ensured and to do so would involve disclosure of information, whether or not agreement has been reached with the service user. In this situation, the staff member involved should seek advice immediately from the HR manager and inform their line manager of this course of action.

The Health and Safety Manager will conform to Health and Safety legislation by informing the workplace of any notification received about any contagious or notifiable disease suffered by any person with whom workers may have had contact during the course of their duties.

In the event of a serious issue arising of a line management nature, (e.g. professional misconduct) supervisors may, within the Policy, raise it with the Operations Manager with or without the staff member's agreement.

There is a legal requirement to disclose information in the event of a Police enquiry which has the back up of necessary legal documentation.

Information and Training

All employees will be provided with this policy document and new employees will receive a copy of this policy on taking up appointment.

The organisation will provide staff training on issues relating to confidentiality and privacy and the contents of this policy in order to ensure that work practices are in line with the requirements of this policy.

Staff working on a regular basis with service users will inform them of this policy document and ensure a copy

is provided to them.

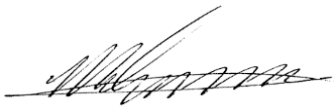
Monitoring

The working of this policy will be monitored regularly, with a record of the number and nature of formal complaints being held by the Chief Executive for monitoring purposes.

Related Policies and Procedures

- Data Protection Policy
- Child Protection Policy
- Vulnerable Adults Protection Policy
- Recruitment and Selection Policy
- Disclosures Policy
- Staff Support and Supervision Policy
- Disciplinary Policy

Date: 1st May 2019



Mark Graves, Director

Reviewed Nov 2021