Calex UK Ltd | Data Protection Policy

DOCUMENT CLASSIFICATION	Internal
DOCUMENT REF	DP01
VERSION	3
DATED	18 August 2026
DOCUMENT AUTHOR	Julia Wilson
DOCUMENT OWNER	Data Protection Lead

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
2	30 October 2024	Julia Wilson	• Responsibility of Data Protection Officer • Purpose of policy added • Updated Data Protection Act to 2018 • Change in Rights to Access Information. Copy of data must be provided within 1 month (3 months in extreme cases)
3	18 August 2026	Julia Wilson	• Removal of Publication of Company Information section as this does not apply

Distribution

NAME	TITLE
All Calex UK Ltd employees	Internal employees

Approval

NAME	POSITION	DATE
David Miell-Ingram	Managing Director	18 August 2026

Calex UK Ltd is committed to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

Purpose of the policy
The purpose of this policy is to ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

Data Protection
The Company needs to obtain and process certain information about its employees to allow recruitment, payment and employment of staff, and comply with its legal obligations. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this the Company must comply with the Data Protection Principles which are set out in the Data Protection Act 2018. In summary these state that personal data shall:

- Be obtained and processed fairly, lawfully and transparently and shall not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive for those purposes
- Be accurate and kept up to date
- Not be kept for longer than is necessary for that purpose
- Be handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

The Company and all employees who process or use any personal information must ensure that they follow these principles at all times. To ensure that this happens, the Company has developed the Data Protection Policy.

Status of the Policy
This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the Company from time to time. Any failures to follow the policy may therefore result in disciplinary proceedings.

Any employee, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the company's Data Protection Officer - dataprocessor@calexuk.com. If the matter is not resolved it should be raised as a formal grievance.

Notification of Data Held and Processed
All employees are entitled to:

- Know what information the Company holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the Company is doing to comply with its obligations under the 2018 Act

Responsibility of Data Protection Officer
The Data Protection Officer is a required appointment in line with applicable data protection legislation (for example the EU General Data Protection Regulation) and has specific responsibilities for the protection of the Personally Identifiable Information (PII) of data subjects.

Responsibilities of employees

All employees are responsible for:

- Checking that any information that they provide to the company in connection with their employment is accurate and up to date
- Promptly informing the Company of any changes to information, which they have provided, e.g. changes of address, telephone number, health status and disabilities to be updated in CIPHR
- Checking the information that the Company will send out from time to time, giving details of information kept and processed about employees
- Informing the Company of any errors or changes. The Company cannot be held responsible for any errors unless the employee has informed the company of them

If and when, as part of their responsibilities, employees collect information about other people they must comply with this policy and the Data Protection Principles.

Data Security

All employees are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party

Employees should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Personal information should be:

- password protected if digital; or saved on digital storage, direct attached storage or network attached storage; or
- Kept in a locked filing cabinet; or
- In a locked drawer

Rights to Access Information

Employees have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should make the request in writing. Employees should make their request to the Data Protection Officer. The Company may make a charge on each occasion that access is requested, although the Company have discretion to waive this.

The Company aims to comply with requests for access to personal information promptly, but will ensure that it is provided within 1 month unless there is good reason for delay. In such cases, the company can take a further 2 months. The reason for delay will be explained in writing to the employee within 1 month of the employee making the request.

Subject Consent

In many cases the Company can only process personal data with the consent of the employee. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the Company processing some specified classes of personal data is a condition of employment for employees. This includes information about previous criminal convictions.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the Company is a safe place for everyone, or to operate other company policies, such as the Sickness Policy and Equality, Diversity and Inclusion Policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to employees, employees will be asked to give express consent for the Company to do this. Offers of employment may be withdrawn if an employee refuses to consent to this, without good reason.
Types of 'sensitive' data, includes:

- race and ethnicity
- religion
- genetics
- health and medical conditions
- sexual history or orientation

The company invites employees to provide this information in CIPHR (Personal Data>Personal Information>Personal Details>Equal Opportunities) for monitoring purposes only. More information about this can be obtained from the Data Processor.

Conclusion

Compliance with the 2018 Act is the responsibility of all employees of the Company. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken. Any questions or concerns about the interpretation or operation of this policy should be taken up with your line manager.

Data Protection Training

All employees are required to complete mandatory Data Protection eLearning helping employees protect personal data and avoid breaches or regulatory penalties, which is accessed via the LEXP platform. Completion of this training is a condition of employment and will be monitored annually

The Data Protection Policy is fully supported and will be monitored to ensure working in practice. The policy will be reviewed every 12 months, considering and taking action to address any issues.

This policy is non-contractual and may be amended at any time to reflect changes in legislation, best practice, or organisational requirements.