Ref	PL/007
Version	5

Information Security and Data Protection Policy (GDPR)

Universal Group processes personal data in relation to its own staff, work seekers and individual client contacts. It is vitally important that we abide by the principles of the General Data Protection Regulation (GDRP) 2018 set out below.

Universal Group holds data on individuals for the following general purposes:

- Staff Administration
- Advertising, marketing, and public relations
- Accounts and records
- Administration and processing of work-seekers personal data for the purposes of work-finding services

The General Data Protection Regulation (GDRP) 2018 requires that Universal Group, as data controller shall process data in accordance with the principles of data protection. Universal Group shall ensure that:

- we will process all personal data fairly and lawfully
- we will only process personal data for specified and lawful purposes
- we will endeavour to hold relevant and accurate personal data, and where practical, we will keep it up to date
- we will not keep personal data for longer than is necessary
- we will keep all personal data secure
- we will endeavour to ensure that personal data is not transferred to countries outside of the European Economic Area (EEA) without adequate protection

General Data Protection Regulation (GDRP) 2018 define 'personal data' as: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Personal data therefore means data, which relates to a living individual who can be identified from the data or from the data together with other information, which is in the possession of, or is likely to come into possession of Universal Group. This incudes, but may not be limited to, a customer, client, employee, partner, member, supporter, business contact, public official or member of the public.

Almost operation performed with data counts as processing, including collecting, recording, storing, using, analysing, combining, disclosing or deleting it. It applies to any processing that is carried out on computer including any type of computer however described, main frame, desktop, laptop, tablet, smart phone etc.

Data should be reviewed on a regular basis to ensure that it is accurate, relevant, and up to date and those people listed in the appendix shall be responsible for doing this.

Data may only be processed with the consent of the data subject, or 'individual' whose data is held. Therefore, if they have not consented to their personal details being passed to a third party this may constitute a breach of the General Data Protection Regulation 2018. By instructing Universal Group to look for work and providing us with personal data contained in a CV work-seekers will be giving their consent to processing their details for work-finding purposes. Where data is intended to be processed for any other purpose, Universal Group must obtain their specific consent. However, caution should be exercised before forwarding personal details of any of the individuals on which data is held to any third party such as past, current or prospective employers; suppliers; customers and clients; persons making an enquiry or complaint and any other third party.

Data shall be processed securely in line with the requirements of General Data Protection Regulation (GDRP) 2018: and shall be 'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.

The general security principles applied by Universal Group specify the way in which we store or transmit information. Every aspect of processing of personal data is covered, not just cybersecurity. Security measures have been devised to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those authorised to do so;
- the data held is accurate and complete in relation to why it is processing; and
- the data remains accessible and usable, i.e., measures are in place to ensure if personal data is accidentally lost, altered or destroyed, it is recoverable it to prevent any damage or distress to the individuals concerned.

These measures are in place to satisfy the requirements under the General Data Protection Regulation (GDRP) 2018 for 'confidentiality, integrity and availability'.

In addition, all employees shall comply with fundamental security measures, for example:

- Computer screens should not be left open by individuals who have access to personal data
- Passwords should not be disclosed
- Email should be used with care
- Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed. They should not be removed from their usual place of storage without good reason.
- Personnel files should always be locked away when not in use and when in use should not be left unattended
- Any breaches of security should be treated as a disciplinary issue.
- Care should be taken when sending personal data in internal or external mail
- Destroying or disposing of personal data counts as processing. Therefore, care should be taken in the disposal of any personal data to ensure that it is appropriate. For example, it would have been more appropriate to shred sensitive data than merely to dispose of it in the dustbin.

It should be remembered that the incorrect processing of personal data e.g. sending an individual's details to the wrong person; allowing unauthorised persons access to personal data; or sending information out for purposes for which the individual did not give their consent, may give rise to a breach of contract and/or negligence leading to a claim against Universal Group for damages from an employee, work-seeker or client contact. A failure to observe the contents of this policy will be treated as a disciplinary offence.

Individuals hold the following rights under the General Data Protection Regulation (GDRP) 2018:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Any requests for access to a reference given by a third party must be referred to the Managing Director and should be treated with caution even if the reference was given in relation to the individual making the request. This is because the person writing the reference also has a right to have their personal details handled in accordance with the General Data Protection Regulation 2018, and not disclosed without their consent. Therefore, when taking up references an individual should always be asked to give their consent to the disclosure of the reference to a third party and/or the individual who is the subject of the reference if they make a subject access request. However, if they do not consent then consideration should be given as to whether the details of the individual giving the reference can be deleted so that they cannot be identified from the content of the letter. If so, the reference may be disclosed in an anonymised form.

Finally, it should be remembered that all individuals have the following rights under the Human Rights Act 1998 and in dealing with personal data these should be respected at all times:

- Right to respect for private and family life [Article 8]
- Freedom of thought, conscience and religion [Article 9]
- Freedom of expression [Article 10]
- Freedom of assembly and association [Article 11]
- Freedom from discrimination [Article 14]

This policy will be reviewed annually, as a minimum.

Signed
Richard Lowe
Managing Director

Ref	PL/007
Version	5

Dated 01/11/2026