2nd March, 2021

**GDPR and Mallory:**

1. Evaluation and risk.
   1. Mallory International MIE (MIE) and its subsidiaries Mallory International Ltd. (MIL) and Mallory International MIC spa (MIC) sell almost entirely to institutions and organisations. Where it holds information about individuals, that is normally in their work capacity. We do not hold home addresses or private details, though we may have mobile numbers.
   2. But circumstances have arisen where our contractual obligations require holding basic details for individuals, in particular parents and families at schools we supply. Sometimes we need to dispatch direct to these individuals. At present, payment is made by the school, so we only need names, addresses and contact phone numbers.
   3. We are developing a virtual book fair product for schools, which would take payment direct from parents, but payment details would be handled by a third party merchant, and Mallory would hold no payment information.
   4. We have a Cardnet machine, which some organisations use for payment. Occasionally the organisation will use a personal credit card. No card details are retained by MIE.
   5. The Companies hold significant personal data in regard to their own staff.
2. Data Control for the Group is the responsibility of the Director (Services), a main board position, who arranges the necessary documentation under Article 30(1) of the UK GDPR.
   1. Accounts staff working for her carry out processing, and documentation under Article 30(2) of the UK GDPR.
   2. Payroll and other internal company procedures are reviewed periodically to ensure GPDR compliance. Payroll and staff data are maintained in secure electronic folders, with access on a need-to-know basis. Training in GDPR procedures is given to personnel who have access.
   3. Information audits are conducted from time to time, but at least annually. This includes review of policies, procedures, contracts and agreements to address areas such as retention, security and data sharing
   4. Current practice is communicated to and checked with customer facing staff.
   5. Privacy notices are reviewed periodically, and in particular at the date of a change in procedures.
   6. There are procedures in place to document and review data breaches.
   7. All records are maintained in electronic form.

Julian Hardinge.