

# Entain Group Data Privacy Policy

## Our Policy

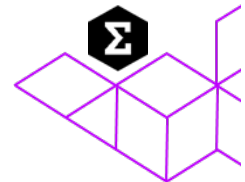
Entain holds and uses personal data from customers, suppliers, you (our colleagues) and others. This Policy, in conjunction with the Data Privacy Guidance Notes, is designed to make sure you understand how to treat and protect the personal data of our customers, suppliers, colleagues and others. It should be read alongside our Cyber Security Governance Policies, standards and procedures.

## Responsibilities

Our role, as the Data Privacy team, is to provide our colleagues with information and guidance on how to comply with applicable data privacy legislation and requirements wherever we operate. However, it is the responsibility of you, our colleagues, to understand and implement the guidance set out in this Policy, where personal data is being processed.

### We must:

- Report any suspected or potential data breaches that puts our customer or employee personal data at risk as soon as a breach has been identified.
  - Breach reporting procedures are managed by the Data Privacy team and overseen by the Data Protection Officers appointed in various jurisdictions (please refer to the Guidance notes for a list of contact details).
- Understand the Cyber Security Governance Policies and Breach Reporting procedures, available within the Guidance Notes.
- Follow our supplier management methodology when procuring supplier services or managing business relationships with suppliers.
- Only transfer personal data electronically, or otherwise, when appropriate measures have been put in place to prevent any accidental loss of data.
- De-identify or encrypt special categories of personal data transferred outside of the company or across public communications networks.
- The following scenarios should be considered prior to any international data transfers being made to ensure the appropriate transfer mechanisms are in place and aligned to our intra group agreement:
  - Countries or territories outside of the EEA, (where the country is recognised by the EEA as having adequate levels of protection for the storage and transfer of personal data for people within the EEA) or is made in compliance with one of the mechanisms recognized by the EEA.
  - Countries that do not have an adequate level of legal protection and must have a Transfer Impact Assessment in place prior to the transmission of data.
  - Any other third countries or territories of other jurisdictions when rules prohibiting or restricting cross-border transfers are imposed under other applicable data privacy laws.
- Only transfer personal data to third parties:
  - If the necessary protective measures set out in the Cyber Security Governance Policies have been put in place.
  - For reasons consistent with the purposes for which the data was originally collected or other purposes authorised by law and/or legislation & regulation.
  - Where written agreements are in place for transfers to third parties for supporting business processes.
- Follow the Group Social Media Policy, owned by the Global Corporate Communications team.
- Only disclose and communicate business-related matters using internal channels approved by the company.



#### **We must not:**

- Collect, process, or transmit data without permission from the Data Privacy team.
- Disclose personal data to unapproved third parties (except to the individual themselves, after checking their identity).
- Discuss, share or post customer or employee personal data via social media, instant messaging applications (e.g. WhatsApp) in public places, with family members or other members of the public - to do so would be in breach of this Policy and may be considered a criminal offence.
- Access or share any Entain personal data outside of what is absolutely necessary to fulfil our work duties.
- Use unapproved third parties (including systems or tooling) to process or store customer or employee personal data.
- Transmit data intentionally or unintentionally in violation of the rules on confidentiality.
- Fail to promptly escalate data subject requests to the correct team.
- Intentionally erase or manipulate personal data.
- Neglect required security measures when processing personal data.
- Use Entain data to make personal profit, cause damage to the company or to harm others.

## **Where can you go for help?**

If you have any queries about this Policy, please either refer to the guidance notes, speak to your line manager, the People team or you can contact the Data Privacy team at [dataprivacy@entaingroup.com](mailto:dataprivacy@entaingroup.com). You can also visit the Data Privacy space on Entain.Me for further guidance.

## **Raising your concerns**

If you suspect a breach of this Policy has occurred or may occur in the future, raise it immediately with your line manager and the Data Privacy team ([dataprivacy@entaingroup.com](mailto:dataprivacy@entaingroup.com)) in the first instance. If that is not possible, please follow the Speak Out Policy. You will not face any adverse consequences for raising a genuine concern in good faith, even if you were mistaken about your concern. Retaliation against a colleague making a genuine report is not tolerated.

## **Who does this policy apply to?**

This Policy applies to everyone working for, or on behalf of, Entain plc and its wholly or majority owned subsidiary companies and joint ventures, such as directors, employees, consultants or self-employed contractors. Entain take breaches of our policies seriously. Failure to comply with this Policy may result in disciplinary action and could lead to civil and criminal prosecutions for noncompliance pursuant to applicable law.

**Policy Owner: Group Deputy General Counsel – Commercial & Privacy**

**Date: September 2025**

**Version Control: 1.7**

**Next Review Date: September 2026**

**Classification: Public**

**Tier: 1**