PART 5

CODE OF PRACTICE FOR CLIENT INFORMATION

A fundamental value of Dentsu is acting responsibly. In the area of servicing clients, this value is reflected in our efforts to ensure the confidentiality, protection and security of client information. This Code defines a number of ethical rules, procedures and safeguards for servicing clients, as adopted across the various agencies that operate within Dentsu.

Management and Organisational Framework

- Client business is handled by separate teams with discrete information, limited data access and defined operational responsibility.

- Client service teams are located in distinct areas or locations, whether operating as separate teams or trading divisions, without access to client specific information held by teams handling competitive clients.

Confidentiality and Prevention of Unauthorised Access

- Non-public information in relation to a client's business, including marketing and advertising strategy, product information, research, communications planning and related work output, is held in confidence, and the maintenance of confidentiality is a matter of priority above and beyond the formal provisions of client contracts.

- Client information remains the sole property of the client and is used by Dentsu and parties working on its behalf solely in relation to the provision and management of contracted services.

- Client records are kept secure, with access to campaign and project data available only as necessary to client service and transactional processing teams.

- Security measures prevent unauthorised internal access to computer systems containing client information. Employees and client teams may only access documents and information for which such access has been granted. Unauthorised access from outside Dentsu is prevented by the use of firewalls and passwords.

- Employees are required to maintain the confidentiality of client information and data.

- Third parties providing operational support such as transactional processing on behalf of Dentsu must adhere to robust data and IT security requirements, including strict confidentiality undertakings that are no less stringent than those imposed by client contracts.

Employee confidentiality

- Employees are educated on the importance of client confidentiality and made aware of our policies and procedures.

- Where necessary, we perform reasonable and necessary due diligence to ensure that new employees do not violate pre-existing confidentiality requirements in the course of their new role.

- Employment agreements for key employees contain clauses obliging employees to protect information about client business both internally and externally.

- Where permissible, employees who fail to uphold these principles may be subject to disciplinary procedures up to and including termination.

IT structure and security

- The IT operating system is protected by a system of firewalls and anti-virus software which automatically intercepts and removes viruses and prevents malware access attempts.

- Users can only login to the network with their passwords which are governed by strong password complexity rules where password renewal is automatically enforced along with password history maintenance. Passwords automatically expire after a set period of days and must routinely be updated.

- External access to systems and client specific applications and data is protected by firewalls and a combination of one-time password token authentication or username and password.

- Access to client computer files is restricted to nominated users and written authorisation is given only by Client Directors.

- IT security procedures are subject to periodic review and audit.

- All client specific extranets are fully protected in line with client security procedures, requirements and external access policies.

- Once obsolete, computer hard drives and portable media are wiped or destroyed.

- Mobile devices are password protected to prevent third parties accessing information. Lost or stolen devices must be reported in order to implement a stop on the device and ensure that data is wiped and confidentiality preserved.

General office security

Our offices represent secure environments for client information and the controls and procedures in place to ensure such a secure environment include:

- Paper records containing confidential information must be filed in locked desks or cabinets.

- Print outs, schedules, general paper records containing confidential information, used as temporary working documents are shredded and then recycled through an accredited third party supplier once we are finished using them.

- No confidential client data may be left unattended on top of desks, printers, copiers or fax machines.

- Further security measures may be implemented where clients have additional specific protocols required for suppliers.

- Access to Dentsu sites is controlled by the issue of security cards. Procedures are in place to ensure the proper issue, activation, return and de-activation of security passes.

Compliance

Dentsu commits resources to ensure the consistent and effective implementation of these procedures across its businesses. Our efforts include:

- Ensuring that our security procedures are periodically reviewed and kept up to date with the confidentiality needs of our clients and in accordance with industry best practice.

- Escalating incidents that adversely affect the security of client information without delay.

If you have any questions on this Code of Practice for Client Information, please feel free to contact compliance@dentsu.com.