Casey GDPR – Employee Personal Data Awareness

Under its GDPR personal data protection obligations, Casey recognises that a fully effective data protection environment will require all employees to follow relevant policies and procedures.

Casey's GDPR compliance requires personal data to be secure. The requirements apply to Employees, unincorporated customers, unincorporated suppliers/subcontractors, residents and tenants and members of the general public.

Non-adherence to the policies and procedures required to meet Casey's data protection responsibilities under GDPR could lead to significant financial penalties to Casey, loss of work and work opportunities and has the potential to allow personal data to be obtained by those that could use it to cause harm to the data subject.

The adherence to these data protection policies is therefore mandatory.

Casey also requires all employees to be vigilant, at all times and to be alert to the need to protect personal data.

All employees are expected to follow these guidelines.

1. Personal data should not be unprotected, if you see personal data in plain view contact the relevant authority immediately to establish whether it is appropriate that this is on view (there may be exceptional circumstances that require this).

2. If you see personal data on or near a printer or photocopier immediately remove this and take it to the relevant authority and tell them where you found it.

3. Personal data secure storage should be locked except when being appropriately accessed. If personal data storage is found in an unsecure state, raise this immediately with the relevant authority.

4. If you are concerned that there may be a risk of personal data being unprotected, contact the relevant authority.

5. Be alert and do not assume that someone else either has or will deal with the issue.

6. Regularly review your workspace and check that personal data is secure – remove phone lists and any other personal data from walls, both in site offices, Head Office and at Regent Street.

7. Password protect documents that contain personal data – keep a separate record of the password (securely).

8. Be extra careful to protect personal data. Avoid sending personal data by email if at all possible. If this cannot be avoided ensure the document has been password protected (see above) before sending and separately email/verbally communicate the password.

9. Do not share personal data with anyone without confirming that the sharing has been approved.

10. Report any suspected data breaches to Group Data Controller

11. Adhere to procedures and policies when they are issued including guide notes

The relevant authority:

- Site manager
- Project/Contracts Manager
- Director
- Group Data Controller or their representative

*Casey includes The Casey Group Limited and its subsidiaries