COHESION

marketing by design

Our data protection statement.

Cohesion is committed to maintaining and improving information and data security within the company and minimising its exposure to risks.

We understand the importance of data protection and have systems and processes in place to manage data within our organisation securely.

It is therefore our policy to ensure that:

The confidentiality of corporate, client and customer information will be assured.

Where freelancers and contractors are used a standard non disclosure agreement is signed before they commence work on the project.

All visitors to our offices must sign in and are accompanied while in our offices.

Management of physical data:

At Cohesion we work in teams to meet our clients' requirements and it is the team leader who is responsible for implementation and enforcing of our data protection policies within their team (staff, freelancers or contractors).

Information may get sent direct to members of a project team and it's every team member's responsibility to look after the data they receive and adhere to our data protection policies.

Data received electronically by clients to progress a project may need to be printed out as the project is progressed. This data will remain within our premises. Should there be a need to take this outside of our premises by a team member, agreement must be given by the team leader.

A record of data taken from our offices by team members is maintained by the team leader. All copies of data will be accounted for and returned to the job bag at the end of a project.

Where ongoing projects are not being worked on all physical data is placed in a job bag and filed away until needed.

Physical information is stored for a period of 3 years when a project is completed unless requested differently by the client.

Files and paperwork that are no longer required after this date are shredded prior to destroying.

If requested by the client secure double shredding at a specialist secure data shredding facility can be arranged.

COHESION

marketing by design

Our data protection policy

Management of electronic data:

Sensitive information (however stored) is protected against unauthorised access through correct software and hardware configuration policies ensuring data access is restricted to authorised staff only. Cohesion operate on Mac OS X system software, which delivers the highest level of security through the adoption of industry standards, open software development, and smart architectural decisions.

With Mac OS X, a security strategy is implemented that is central to the design of the operating system, ensuring that your system is safe and secure.

Using open source methodology makes Mac OS X a more robust and secure operating system, because its core components have been subjected to peer review for decades.

All ADSL/Broadband hardware is configured with full security enabled, again allowing access to such devices and services to authorised staff only using the correct security policies.

All computers have a unique user login. Users need to login to access their email. A further login process is then required to access the file server. The file server has different volumes for storing different types of information. Access to these volumes is by membership of password-protected groups.

Remote access by clients and suppliers is via a secure login to a specific volume only.

The server is backed up daily by DAT tape and the DAT tape stored in a secure fire safe. Remote back-up of users' email occurs twice a week by DAT tape and the tapes stored in a secure fire safe.

Data no longer needed gets archived from the file server onto DVDs and stored securely. These DVDs are stored for a period of 10 years unless otherwise requested by the client.

Should data need to be copied to either a CD/DVD, memory stick or any other portable device, this is overseen by the team leader. When finished with the portable device will be returned to the team leader who will destroy the device or organise removal of the data.

Approval from the team leader must be sought before any data is copied to a data storage device.

Only Cohesion email accounts are used to receive and send emails to clients. Where staff work remotely from our offices they will access their email from a secure web mail application provided by our service provider.

Only the authorised user of an email account will access the email in their account unless specified by the team leader in order to cover circumstances such as holiday. Should this happen then the password of the account being accessed by other users will be reset when the authorised user returns to work.

myTsafe

Where ultra security is required for specific projects we use myTSafe – an ultra secure online document store, which also allows secure e-posting into accounts removing the need for email. Documents can also be shared with other myTSafe users. The service is hosted at The Bunker which offers:

Physical security: Located deep underground in an ex-Ministry of Defence nuclear attack-proof bunker built to house computers.

Electronic security: State of the art digital security, managed by people who are among the foremost computer security experts in the world.

Procedural security: All procedures and practices are of military standard or better. All employees undergo intensive security screening carried out by an approved specialist company. Where staff work on data at home, the data is transferred electronically by secure login to our server and then once copied back deleted from the computer being used at home.

COHESION

marketingbydesign

Our data protection policy

Management of electronic data