mcc digital

GDP Compliance Statement

GDP Compliance Statement

Welcome to MCC Digital's statement on GDPR and Data Security. This document should be read in conjunction with our main Privacy Policy.

GDPR Principles we Operate by
Accountability: We are committed to the principles of the GDPR by adopting the concept of 'data privacy by design' within our operational model. We remain accountable by having detailed policies and systems in place as well as a Data Protection Officer to oversee our overall compliance to data protection regulations including the management of access rights requests. Our policies are regularly reviewed and updated, and our staff are periodically trained on data protection and security throughout the year
Transparency, Fairness and Lawfulness: We process data with data subjects' interests in mind and ensure that we approach processing activities with transparency to maintain fairness in what we do. This way we can be sure that we are processing data lawfully. We have a robust process in place to allow us to deal efficient with any access requests we may receive.

Data Integrity and Confidentiality: We hold data on secure systems, and we are cyber essentials plus certified. We can provide evidence of our certifications on request.

Information security and integrity is key to our smooth operation, and we have dedicated cyber security team who protect our systems. We also have an Incident Response Team on hand to support us in the event data may become compromised.
Data Minimisation and Data Storage: We will not keep data for longer than is necessary and only keep data if there is a lawful basis which allows fair retention. When we do need to remove data from our possession, we do so by using industry approved standards So the disposal or anonymisation is thoroughly complain.

Data Accuracy: Keeping data accurate is very important to us and we train our staff to ensure they are maintaining data to a high quality and with all the facts available.

GDP Compliance Statement

Purpose Limitation: We use the data we attain for a specific purpose. This means that data is not processed for any alternative reasons other than what the data was originally collected for.

The tables below explain our stance on different operational areas of our business, so that you can easily see the standards we work by. If you have any further queries about any topics raised in this document, please contact our Data Protection Officer on GDPR@MCCDigital.com for further assistance and clarity Physical Security of our sites.

Buildings	Reception areas are staffed 24/7 and door access control systems are in place throughout the building and all entrances are monitored by CCTV.
Secure areas	Secure access areas are protected by entry controls to ensure only authorised staff can enter via an access control pad. Access rights are removed when staff move roles and access rights are limited to necessary personnel required.
Business Continuity	A BCP/DR policy has been implemented. A full annual DR test is conducted and individual components are tested at on a regular basis. All necessary remediation has been carried out.

Cyber Security and Compliance	Data Protection and Cyber Security is our #1 priority at MCC Digital Group. We hold multiple accreditations such as Cyber Essentials Plus. We heavily invest in People, Processes and Technology to ensure that the protection of our customer and employee data remains the top priority.

mcc digital

GDP Compliance Statement

Software and Applications	• Software applications are managed through a standard Agile software develop methodology. Once a change is completed, end to end testing is performed to ensure the accuracy of the change and the existing system functionality. • Only approved software is manged and patched centrally and permitted on user machines which is managed through Jamf. • Software is then packaged and released. Security and vulnerability testing is integral to the development lifecycle. • All operating systems in place are fully supported and patched. • We use desktops and laptops which use MacOs with our cyber security updates being installed automatically. • No sensitive information is stored on non-compliant systems.

mcc digital

GDP Compliance Statement

Network Access	• Internal network access is controlled through internal Active Directory security. • Access to applications is made via https secure internet browsers. Internal systems can only be accessed within the secure Corporate network. • A strong password policy has been implemented with complexity and Multi-Factor Authentication with Conditional Access to protect against phishing and malware attacks. • All access is granted on the principle of 'Least Privileged Access'.
VPN Access	• Remote working is enabled for approved employees and is enabled via secure encrypted VPN with multifactor authentication.
Encryption	• All Data at Rest and in Transit is encrypted. All databases, software and hardware/devices are protected with high levels of encryption. Encryption keys are managed with strict policies and procedures. The keys are stored in a secure location which is only accessible to database admins.

mcc digital

GDP Compliance Statement

Monitoring and Testing	• IDS, IDP and SIEM provide monitoring for the network 24/7 and Data Loss Prevention technology and strategies provide protection against accidental and malicious data loss and cyber attacks. • Vulnerability Management and Penetration Testing are integral to our testing strategy. • All patches are governed by the change control process which includes evaluation, testing and deployment. • A standard build procedure ensures that all default admin and back door accounts are removed.
System Updates	• We update systems in line with Microsoft and Cyber Security best practices to ensure that all systems are patched and that we are always using the most advanced technical and organisational controls and tools available.

mcc digital

GDP Compliance Statement

Data Back Ups	• Data is backed up daily to redundant backup locations and all backups are encrypted. • Measures are in place to ensure that the business can continue to function should a compromise occur. • Data is backed up to physical media stored offsite at our secure data backup facility which is owned by the group and secured with CCTV, physical locks and limited access controls. • The data restore process is tested monthly or as required. • Performance monitoring and file integrity monitoring is in place to ensure our business continuity plan can take full effect.
Cloud Providers	• We may use cloud storage facilities for processing and storing data and when we do this, we ensure that the security is maintained and tested regularly. • Our CRM is built on cloud-based infrastructure. • All data resides in the EU or UK area and no data is transferred out of the EEA.

mcc digital

GDP Compliance Statement

General	• All networks have firewalls, antivirus and EPP & EDR protection in place which is deployed on all endpoints to detect, alert and neutralise any threats. • Any applications accessible from the internet are constantly safeguarded to prevent the existence and exploitation of web application vulnerabilities such as cross-scripting or SQL injection. • External connections are protected with enterprise, resilient firewalls and dedicated security monitoring including SIEM, IDS and IDP. • All internet access is controlled by a dedicated web filtering appliance which restricts the types of traffic and URLS. • Firewalls and monitoring control and monitor traffic entering and leaving the organisation. • Enterprise Security Monitoring has been implement for 24/7 visibility & protection.

mcc digital

GDP Compliance Statement

Third Party Security . . .

	• All contractual IT security requirements are in place with any third parties we use which ensures the relationship remains subject to GDPR compliance. • Where necessary, our contract with them includes Data Processing Terms or terms are built into our products terms and conditions. • We also use alternative data protection safeguard mechanisms where appropriate in the form of standard contractual clauses where required. • Our CRM systems is Capsule which is PCI-DSS compliant. We can confirm that they also have a dedicated security team which regularly tests and verifies that all controls are operational. • All SCapsule data resides in the Primary & Secondary Data centres in the UK. All group data bases reside in a primary and secondary data centre which are both based in the UK. • MCC Digital's data is segregated from other Salesforce customers.

mcc digital

GDP Compliance Statement

Staff Security	• All staff are screened prior to their engagement and interviews are face to face where possible. • All staff get an induction focused on data protection and security plus all our staff's CV statements and qualifications are checked for validity before the offer of employment can commence. • Each staff member is issued with an Employee Handbook which we regularly review and update where necessary. • We update our staff when additions and updates are made. • A restrictive covenant is signed by staff prior to employment and a confidentiality agreement is signed on the first day of employment. • All staff receive security training as part of their induction which is reinforced periodically during training sessions and presentations. • When an employee leaves the business, all accounts and access is suspended immediately, blocking all access to our systems and buildings. • A clear desk policy is in place across the group and staff know to lock screens when they are away from their desks for any period. • We operate policies for data security for our remote and field workers so that integrity is always maintained. • Staff are not permitted to store any data via removable media (USB's) or on device hardware.

mcc digital

GDP Compliance Statement

Data Retention and Disposal . . .

Data Retention	• All data retention is handled in line with our retention policy. We are committed in taking a practical approach in line with legal, contractual and commercial requirements relating to the ownership, retention and disposal of information relating to our business activities within the UK and Ireland. We tend to keep our client data for 2 years until the contract end date.
Data Disposal	• As a company we have made a conscious effort to become more digitally focused and we steer away from paper records wherever possible. • Confidential waste bins are located on each floor for confidential paper waste and this is securely shredded by a vetted third party who provide a certificate of destruction upon completion. • We have a hardware disposal policy in place which ensures that all hardware is commercially wiped before final destruction via an accredited third party who also provide certificate of destruction.

GDP Compliance Statement

MCC Digital has a dedicated representative who can be approached for any questions, comments and requests regarding this privacy policy or our Data Privacy Management System. Frequently asked questions about or GDPR compliance can be accessed here. Our Data Protection officer welcomes communication around our policies and practices and they can be directly contacted on the details below, which are also publicly available on the ICO register. You can also write to us at MCC 27-31 Earle Street Newton-le- Willows Merseyside WA12 9LW. GDPR Oversight Team: GDPR@mccdigital.com Data Protection Officer: m.ffleming@mccdigital.com If you're not satisfied with our response, or believe we're not processing your personal data in accordance with the law, you can approach the UK regulator or further guidance at www.ico.org.uk/concerns