Data Protection and Confidential Information Policy

ARC:MC Limited is a company registered in England and Wales, with company number reg no. 7083299. Our head-office contact phone number is 020 3411 2571, you can email us at info@arcmc.co.uk and our postal address is: 39 Moreland Street, London, EC1V 8BB.

This policy describes how this personal data and confidential project data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law. Our BYOD Policy, Password Policy and Administrative Access Policy documents should also be reviewed alongside this policy document. A copy of these can all be made available on request.

This data protection and confidential information policy ensures ARC:MC:

- Complies with data protection law and follows good practice
- Protects the rights of customers, suppliers and business contacts
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

This policy applies to:

- All staff of ARC:MC
- All contractors, suppliers and other people working on behalf of ARC:MC

Confidential Project Information

Confidential Information is any information that is not generally available to the public and is proprietary, secret, or sensitive in nature. ARC:MC have been completing projects which are classified as confidential for many years. These are typically conducted with NDAs (Non-Disclosure Agreements) in place.

Employees must ensure that confidential information is not disclosed, copied, or removed from the organisation's systems or premises, except where necessary and authorised for performing their job duties.

Confidential information should be used solely for the purpose of carrying out the organisation's business and in compliance with applicable laws and regulations. The unauthorised use, copying, or distribution of confidential information is strictly prohibited.

Employees should treat confidential information with the utmost care and not disclose it to any unauthorised persons or third parties except as required by law. Employees must ensure that confidential information is not discussed in public areas, should be locked or secured when not in use and appropriately destroyed using a confidential waste removal firm.

Data Protection & GDPR

As a Data Controller, we gather and use certain information about individuals in order to conduct necessary project, contract and employment deliverables. This can be in the form

of names, emails, phone numbers, etc. The majority of data is provided to us directly from the individual or business it is referring to. We shall only use personal data for the purpose for which it was received for example payment processing, invoices or internal quality assurance systems. The persons we may hold data on can include customers, suppliers, business contacts and other people the business has a relationship with or may need to contact to provide our services.

This policy applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act or GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Bank Details
- Plus any other information relating to individuals

The Data Protection Act 1998 and the EU General Data Protection Regulation 2018 describe how organisations — including ARC:MC— must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

The EU General Data Protection Regulation (GDPR) is a significant piece of European legislation which came into force in 2018. It builds on existing data protection laws, strengthening the rights that EU individuals have over their personal data, and creating a single data protection approach across Europe. This legislation stills effects the UK post-Brexit - especially our business where we process data for individuals within the EEA and EU.

To comply with The Data Protection Act and EU General Data Protection Regulation ARC:MC have numerous processes and security measures in place to ensure our compliance regarding the handling of personal information. The legislations, and in turn our procedures, are underpinned by the following important principles on personal data:

1. Be processed fairly and only for specific, lawful purposes
2. Be obtained with consent
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Regarding EU Citizens, not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Data protection risks

This policy helps to protect ARC:MC from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them and have a right to withdraw consent.

- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Areas of responsibility

Everyone who works for or with ARC:MC has some responsibility for ensuring personal and confidential project data is collected, stored and handled appropriately. They must ensure that it is handled and processed in line with this policy, NDAs and all data protection principles. ARC:MC shall provide our team with regular IT Security, Confidentiality and Data Protection Training to help ensure awareness around this issue.

As a Data Controller ARC:MC's main responsibilities are to:

- Review all data protection procedures and related policies, in line with an agreed schedule and provide transparent information to all.
- Ensure that voluntarily (opt-in) consent has been obtained by all who's data ARC:MC hold.
- Deal with requests from individuals to see the data ARC:MC holds about them within the 21 day guideline.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data – including a Data Processor Agreement when necessary.
- Perform regular data audits to ensure retention periods and suitable erasure processes of data no longer necessary to hold.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Train our team in data security and ensure an awareness of data protection law and how to identify breaches or DSARs.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Should a data breach occur we shall report it to the ICO within 72 hours of occurrence and implement a risk response plan immediately.

General Contractor Guidelines are as follows:

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should never be shared informally.
- Contractors should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used in line with our Password Policy and Multifactor Authentication should be implemented.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Should a breach of data occur the Data Controller must be informed immediately
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Contractors should request help from ARC:MC if they are unsure about any aspect of data protection.

Data Storage & Use

Practically, personal data is of no monetary value to ARC:MC, however, it is when personal data is accessed wrongly and used that it can be at the greatest risk of loss, corruption or theft. These rules describe how and where data should be safely stored. Any questions about storing data safely can be directed to ARC:MC as the data controller.

- When not required, paper or files should be kept in a locked drawer or filing cabinet. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
- Should you make paper printouts make sure they are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required, using our specialist confidential waste removal service.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data/Devices should be protected by strong passwords that are changed regularly and never shared.
- If data is stored on removable media these should be encrypted and also kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- When working with personal data, you should ensure the screens of computers are always locked when left unattended.
- Personal data should not be shared informally.
- Personal data should never be transferred outside of the UK or European Economic Area.
- You should not save copies of personal data onto personal computers/devices.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Accuracy

The law requires ARC:MC to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort ARC:MC should put into ensuring its accuracy. It is the responsibility of all contractors who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

We shall help ensure accuracy with the following:

- Data will be held in as few places as necessary.
- Always access and update the central copy of any data.
- Data shall only be used for its intended purpose.
- Data minimisation should occur (we only collect the data we need)
- ARC:MC will make it easy for data subjects to update the information held about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by ARC:MC are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access/a copy of it.
- Be informed how to keep it up to date.
- Have the right to be forgotten
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a data subject access request. DSARs from individuals should be made by email, addressed to the data controller at emily.mcneal@arcmc.co.uk.

The data controller will aim to provide the relevant data within 21 days in a portable format. There is no charge for standard DSARs. The data controller will always verify the identity of anyone making a subject access request before handing over any information and ensure the protection of other's data during the process.

Please note for instances involving any EEA data request we shall act as principal contact, but shall be supported by an EEA GDPR representative. You can contact are representative via this email : art-27-rep-arcmc@rickert.law

Should you have a complaint about how your data has been handled by ARC:MC you can register a grievance with our local regulatory authority the ICO here: https://ico.org.uk/make-a-complaint/

Disclosing data for other reasons
In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, ARC:MC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.