

We are writing to let you know that we have updated our data protection policy. The changes have been made in order to comply with the General Data Protection Regulation (known as GDPR), which gives you more control over how your data is used and how you are contacted. C Fullard Metals Ltd take the protection of your data very seriously and safeguard as much as we possibly can.

C Fullard Metals GDPR Data Compliance Statement

We do not share or sell your personal data to third parties.

Your data will be processed lawfully, fairly and in a transparent way limited only to what is necessary in relation to the purpose.

We retain your personal information for no longer than is legally necessary and securely erase all information when no longer needed.

We collect a range of personal information relating to you including your name, email address, phone number and any other personal information that you choose to provide us when you make contact with us.

If you are a customer or supplier, we will use your information to process invoices, payments and to communicate with you. We will keep information such as your transaction history.

We may use Experian obtain credit checks and references for debt collection and insurance purposes.

The below technical measures have been taken in order to protect personal data from unauthorised access:

- Antivirus software that provides malware protection
- Antivirus software that provides email and browser protection
- Company computer network firewall protection
- Daily backup of data, automatically enforced
- Wi-Fi network is password protected
- Remote access to company computer network is possibly only via a virtual private network (VPN)
- Login to privileged accounts is possible only from dedicated devices and limited to authorized persons only
- Access to sensitive/personal data is controlled and limited only to persons that need to access them
- Data leakage prevention software to protect sensitive/personal data
- Procedures for monitoring, detecting, analysing and reporting of security incidents are developed and communicated within the company