MALLING REPAIR SERVICES LTD
GDPR 2018
POLICY

Data on Malling Repair Service's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorized access to confidential information under the regulations of the GDPR 2018.

Users are expected to adhere to the regulations and training provided when dealing with information data that is confidential and to proeccess any data in line with the companies practises and proceedres that have been implemented under the rules and regulations of the GDPR 2018.

Users must not send, upload, remove on portable media or otherwise transfer to a non-Malling Repair Service system any information that is designated as confidential, or that they should reasonably regard as being confidential to Malling Repair Service, except where explicitly authorized to do so in the performance of their regular duties and the correct, recording permission has been sort.
Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with Malling Repair Service's safe password policy.

Users who are supplied with computer equipment by Malling Repair Service are responsible for the safety and care of that equipment, and the security of software and data stored it and on other Malling Repair Service systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.
All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.
Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into Malling Repair Service's systems by whatever means and must report any actual or suspected malware infection immediately.

Unacceptable Use

All employees should use their knowledge and GDPR training regarding what is unacceptable use of Malling Repair Service's systems. The activities below are provided as examples of unacceptable use, however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.
All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations 2018.

All activities detrimental to the success of Malling Repair Service. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.

All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).

All activities that are inappropriate for Malling Repair Service to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment, data briech.

Circumventing the IT security systems and protocols, which Malling Repair Service has put in place.

Enforcement

Malling Repair Service will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include the termination of their employment.
Use of any of Malling Repair Service's resources for any illegal activity will usually be grounds for summary dismissal, and Malling Repair Service will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

Signed……N Mepsted……..
Nigel Mepsted (Director)