

**Personal data** means data which relate to a living individual who can be identified – such as, but not limited to:

* A person’s name
* Their address
* Telephone numbers
* Occupation
* Physical characteristics
* Pseudonyms
* Ethnicity
* Physical or mental health records
* Political opinion
* Religious beliefs
* DBS. This is the results of a criminal records check
* The definition is also technology neutral.  It does not matter how the personal data is stored – on paper, on an IT system, or on a CCTV system etc.

**Dos**

* Always follow JPS Projects Limited security procedures to ensure people’s personal data is protected. The procedures include but are not limited to:
* Password controls – regularly change your password and do not share with anyone. Please refer to our IT Policy
* Passwords are unique to each user and must be changed regularly to ensure

Confidentiality. Passwords must be kept confidential in line with the IT Policy and must not be made available to anyone else

* Always **lock** computers, tablets and PDAs when not in use, when you leave your desk lock or shutdown your computer
* **Building security** – keep doors shut at all times
* Shred documents with personal data on when finished with them
* Avoid careless talk about people in public places or on a mobile phone such as gossiping or disclosing medical conditions
* Explain to customers why we need their personal data i.e. “please can I have your mobile number so the Operative can ring you when they’re on their way” or “we would like your email address so we can contact you in a more convenient way”

• When sending or saving a document containing personal data, always password protect the document. If sending via emails do **not include the** **password in the email**. Communicate separately by email, text or a phone call

• Only share personal data with people and third parties authorised by the Executive Directors and Data Protection Officers

• Say “no” if you are not sure that you should share personal data, and seek the advice of your line manager

• Keep your employee details up to date

• Keep customer details up to date

**Don’ts**

• Don’t leave unattended or visible any documents with personal information on desks, in vans, customers’ homes or public places

* Don’t leave job sheets lying around, particularly in customers’ homes or other public places
* Don’t discuss or record any private information relating to a customer, unless it is specifically related to the job. This includes on social media and on text messages
* Don’t include people in photographs of work unless it is impossible not to i.e. a wide shot of a communal area with passers-by in the background that can’t really be identified or we have prior consent from the person being photographed

**Breaches**

* Any breaches or suspected breaches of data protection must be reported immediately to Sarah McGlynn Office Manager

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Trade/Position:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**I agree to abide by the security procedure as imposed by**

**JPS Projects Ltd under the GDPR Data Protection Act 2018**

**Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**