Holst
WORKPLACE EFFECTIVENESS

# INFORMATION SECURITY POLICY – HOLST

Holst takes Information Security seriously alongside our other Data Protection policies.

The security measures we have put in place ensure that:

- data can be accessed, altered, disclosed or deleted only by those who have been authorised to do so (and that those people only act within the scope of the authority given to them);
- the data we hold is accurate and complete in relation to why we are processing it; and
- the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, we have systems in place to recover it and therefore prevent any damage or distress to the individuals concerned.

These form the 'confidentiality, integrity and availability' or CIA as stated under the GDPR.

**PHYSICAL SECURITY**

- Access to our premises and equipment is not given to anyone outside our organisation without supervision.
- We have business continuity arrangements to protect and recover any personal data we hold; and
- We undertake periodic checks to ensure that our security measures remain appropriate and up to date through our quarterly GDPR meetings.
- The quality of doors and locks, and the protection of our premises by alarms, and secure entry are maintained.
- Visitors are supervised when they are on site at all times by a member of our team.
- We dispose of any paper and electronic waste in line with GDPR regulations.
- We keep IT equipment, particularly mobile devices, secure.

**COMPUTER SECURITY**

- We have a firewall and virus-checking on our computers.
- Our operating system is set up to receive automatic updates.
- We protect our computers by downloading the latest patches or security updates, to help overcome vulnerabilities.
- We only allow our staff access to the information they need to do their job and don't let them share passwords.
- We encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.

+44 (0)203 111 9292
hello@weareholst.com
www.weareholst.com

- We take regular back-ups of the information our computer system and keep them in a separate place so that if we should lose our computers, we don't lose the information.
- We securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- We regularly check the data we hold and delete any "old" data.

**EMAIL SECURITY**

- We will check the right email address is selected before sending personal data.
- We will ensure that we use blind carbon copy (bcc), not carbon copy (cc) when sending to multiple addresses so as not to reveal recipient addresses.
- Group email addresses will be checked before sending to ensure the message goes to the appropriate audience.
- We will only send a sensitive email to a secure recipient.

**FAX SECURITY**

- We do not fax personal data

**COLLEAGUE TRAINING AND SECURITY**

We have trained our colleagues as follows:

- they know what is expected of them in terms of Data Protection and Information Security
- to be wary of people who may try to trick them into giving out personal details;
- they are aware that they can be prosecuted if they deliberately give out personal details without permission;
- to use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
- not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
- not to believe emails that appear to come from our bank that ask for account, credit card details or passwords (a bank would never ask for this information in this way);
- not to open spam – not even to unsubscribe or ask for no more mailing – we ask them to use the "report spam and unsubscribe" and/or delete permanently

- everyone should comply with information security procedures including the maintenance of data confidentiality and data integrity.
- each colleague is responsible for the operational security of the information systems they use
- each system user will comply with the security requirements that are in force and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard
- any information being transferred on a portable device (mass storage device, or laptop, for example must be encrypted in line with industry best practices and applicable law and regulations)
- any breaches to the policy will be reported to the Directors and Data Protection Officer and a full investigation will be carried out