

Supplier Use of Device Policy

Tecknuovo Limited

INTERNAL

1 Introduction

- 1.1 Tecknuovo is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.
- 1.2 This policy supplements Tecknuovo's other policies and procedures, which together place obligations on suppliers to take appropriate measures to safeguard Tecknuovo information against unauthorised or unlawful use, accidental loss, destruction or damage, by extending and/or clarifying these obligations for suppliers and their staff who are required to use their own devices when delivering services for projects for Tecknuovo.
- 1.3 The purpose of this policy is to protect Tecknuovo's confidential, commercially sensitive and personal information and to ensure Tecknuovo can comply with its legal and regulatory obligations, including those regarding data protection, record retention and audit by setting out the circumstances in which Tecknuovo may monitor your use of its systems; access, retrieve, remove and destroy data on supplier device; and the action Tecknuovo may take if you fail to comply with the obligations contained within this policy.
- 1.4 Tecknuovo expressly reserves the right to amend or remove the policy at any time. Changes made to this policy will be notified to suppliers via email.

2 Definitions

For the purposes of this policy:

breakdown	means any failure or stoppage in the proper mechanical function of the Tecknuovo device;
business information	means business-related information other than personal information regarding customers, clients, suppliers and other business contacts of Tecknuovo;
confidential information	means trade secrets or other confidential information (either belonging to Tecknuovo, its customer and/or to any third parties) that is owned and/or processed by Tecknuovo;
device	means all electronic devices, including laptops, tablets, personal digital assistants and other hand-held or portable devices, smartphones, and any other applications or technology that are used by any supplier and/or their staff

to access, store, create, copy or transmit Tecknuovo information;

IT network

means the IT network of Tecknuovo and/or its customers;

IT systems

means the IT systems of Tecknuovo and/or its customers;

personal information

(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

secure area

means the Supplier's offices, Tecknuovo's offices, and/or any customer premises the Supplier has agreed to deliver services from;

statement of work

means any statement of work the Supplier enters into with Tecknuovo for the delivery of services to Tecknuovo;

supplier device

means any device utilised by the Supplier and its staff in the delivery of services to Tecknuovo and which is owned, leased and or hired by the Supplier (and is not owned or supplied by Tecknuovo or on its behalf);

Tecknuovo device

means any device utilised by the Supplier and its staff in the delivery of services to Tecknuovo and which is loaned to the Supplier by Tecknuovo (whether owned, leased, or hired by Tecknuovo or on its behalf) and which includes any peripheral or accessory supplied with such device;

Tecknuovo information

means business information, confidential information, and personal information relating to Tecknuovo staff, customers and suppliers;

use

means to receive, store, transmit, process, access, read, analyse, disclose, share, print, copy, reproduce, extract, modify, adapt, incorporate or use Tecknuovo Information in whole or in part in any manner whatsoever.

3 Scope and data protection

- 3.1 Tecknuovo information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of Tecknuovo, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

- 3.2 This policy applies to all suppliers and their employees, officers, sub-contractors, contractors, interns, volunteers and apprentices (staff).
- 3.3 All Suppliers and their staff must be familiar with this policy and comply with its terms.
- 3.4 This policy supplements Tecknuovo's IT Security Policy, Supplier Code of Conduct, and other policies and privacy notices relating to the handling of confidential and personal information and the contents of those policies must be taken into account, as well as this policy.
- 3.5 All Suppliers and their staff who use any devices for Tecknuovo projects must comply with Tecknuovo's IT Security Policy and the data privacy standard detailed in paragraph 15 (Data privacy standard) of this policy.
- 3.6 This policy will entitle and enable Tecknuovo access to and process personal information on any device. Tecknuovo relies on the following lawful bases for that processing:
- 3.6.1 it is necessary for Tecknuovo to comply with its legal obligations to protect the personal information of its staff, customers and third parties; and
 - 3.6.2 it is necessary for the purposes of Tecknuovo's legitimate interests, namely, to protect its Tecknuovo information and the security of its systems.
- 3.7 We will review and update this policy in accordance with our data protection and other obligations. It does not form part of any supplier contract and we may amend, update or supplement it from time to time. We will circulate any new or modified policy as and when it is adopted.

4 Obligations regarding information security

- 4.1 In permitting suppliers to use supplier devices for Tecknuovo projects, Tecknuovo requires all suppliers to exercise all necessary care, take certain precautions and be responsible when using such devices to connect to IT systems and/or to access Tecknuovo information.
- 4.2 In order to protect Tecknuovo information, suppliers are required to comply with the obligations set out below at all times.
- 4.3 If suppliers do not comply with this policy, Tecknuovo may revoke its permission for a supplier to use its own devices for Tecknuovo projects and may take other appropriate action (see paragraph 20 (Failure to comply with this policy) below).
- 4.4 If you have any questions about this policy, please contact the Associate Management team or the Tecknuovo Delivery Hub.

5 Tecknuovo information

- 5.1 All Tecknuovo information should be considered to be commercially valuable and you must protect it from loss, theft, misuse, inappropriate access, modification or disclosure. Suppliers should exercise an even higher degree of caution when accessing or working with sensitive information, in respect of which the impact of loss or unauthorised access may be even more serious than would ordinarily be the case. Suppliers are referred to the confidentiality obligations set out in their contract with Tecknuovo.

5.2 Supplier obligations concerning data security generally (including regarding technical security measures and organisational security measures) are detailed in Tecknuovo's IT Security Policy.

6 Supplier devices

6.1 Tecknuovo will only consider permitting suppliers to use their own devices in accordance with this policy if it is listed and supported below (such list will be maintained and updated from time to time):

6.1.1 Mobile phone

6.1.2 Smart phone;

6.1.3 iPhone;

6.1.4 iPad;

6.1.5 Blackberry;

6.1.6 Laptop and/or Notebook;

6.1.7 Tablet;

6.1.8 Desktop PC

6.2 Before any staff of the Supplier connect devices utilised on projects to the IT systems and/or to access Tecknuovo information in accordance with this policy, a supplier must and shall implement technical security measures as Tecknuovo reasonably require, including:

- (a) measures set out in the Tecknuovo IT and Security Policy; and
- (b) measures that meet the standards required of the Cyber Essentials requirements for IT Infrastructure covering firewalls, secure configuration, user access control, malware protection, and patch management (please see Clause 9.2 for more information and a link to the current requirements).

6.3 The Supplier shall ensure no member of its staff are permitted to use any supplier device and shall not allow its staff to connect to IT systems and/or to access Tecknuovo information unless and until such device complies with clause 6.2 above.

6.4 Tecknuovo reserves the right to retract and permission for any such device to connect to the IT systems and/or access Tecknuovo information where it is of the reasonable opinion that any supplier device is or may be capable of being used in a way that may breach this policy.

6.5 The Supplier is expressly prohibited from saving and/or storing Tecknuovo information and any output of the services and deliverables pursuant to a statement of work (**SOW Materials**) to local drive of the Supplier device, any external drive or storage device, or any other internet or i-cloud based productivity applications, document management, and/or storage systems of the Supplier. All SOW Materials must be prepared, processed, stored and saved only

within the IT systems which Tecknuovo grants the Supplier access to during any statement of work, unless otherwise expressly agreed in the statement of work.

- 6.6 To the extent that any SOW Materials are prepared, processed and or stored in the Supplier's business email accounts, the Supplier shall ensure that unless its emails are sent and received using end-to-end encryption services, the Supplier shall not send confidential information via its business email accounts unless with the written consent of Tecknuovo. Dependant on the nature of the services and commercial sensitivity of the project Tecknuovo may require the Supplier utilise an email account providing end-to-end encryption services or such other enhanced security protection for a statement of work and which must be used for all email communication relating to the statement of work (**Tecknuovo Email**). If the Supplier is required to use Tecknuovo Email, the Supplier shall and shall ensure the staff shall only utilise such Tecknuovo Email for the duration of the statement of work and thereafter until such time as Tecknuovo deactivates the Supplier's access to such Tecknuovo Email. The Supplier shall comply with any terms of use of the Tecknuovo Email notified to the Supplier upon activation of any the Tecknuovo Email.

7 Tecknuovo devices

- 7.1 Dependant on the commercial sensitivity of the services to be delivered and or any sensitivity in the Tecknuovo Information to be accessed by the Supplier to Tecknuovo under a statement of work, Tecknuovo may require the Supplier utilise Tecknuovo devices to deliver the services.
- 7.2 Any requirement to use Tecknuovo devices will be set out in the statement of work and the Supplier shall use such devices in accordance with this policy. The Supplier may be required to pay a fee for or loan deposit in respect of the loan of the Tecknuovo devices for the duration of the statement of work, the terms of which shall be set out in the relevant statement of work.
- 7.3 Tecknuovo devices will be loaned to the Supplier for the duration of the statement of work, however the Supplier acknowledges and accepts that Tecknuovo may demand the return of any such devices on giving verbal notice to the Supplier, which shall only occur if the statement of work ends earlier than expected or is otherwise terminated by any party pursuant to the statement of work. The Supplier will comply with any instructions issued by Tecknuovo as to the method of and timing of the return of the Tecknuovo device and with particular regard to any timescales required.
- 7.4 Tecknuovo shall notify the Supplier whether the Supplier is required to collect any Tecknuovo device from any secure area (in accordance with the instructions as to date and time of collection) or whether such device will be delivered to the Supplier's offices (the Supplier ensuring that its staff will be present to receive delivery of and sign any delivery note for such Tecknuovo device at the date and time of delivery instructed by Tecknuovo).
- 7.5 Title and all rights to the Tecknuovo device shall at all times be vested in Tecknuovo (or the customer as the case may be) (**Owner**) and the Supplier acknowledges that it has no right, title, or property in the Tecknuovo device.
- 7.6 Risk in the Tecknuovo device shall pass to the Supplier upon delivery to the Supplier or upon collection by the Supplier (as applicable) and shall not revert back to the Owner until the Tecknuovo device is back in the Owner's possession or control, notwithstanding the expiry of or earlier termination of the statement of work.

- 7.7 The Supplier shall be responsible for arranging insurance cover, on a full replacement basis, in respect of any Tecknuovo device against the risks of loss, theft and damage beyond economic repair. The proceeds of any claim in respect of such insurance shall be held by the Supplier on trust for the Owner.
- 7.8 The Supplier shall and shall ensure that its staff do not or do not allow to be done any act or thing that may reasonably be expected to prejudice or endanger the Owner's property or rights in the Tecknuovo devices.
- 7.9 All Tecknuovo devices delivered to the Supplier should be configured and customised by the Owner so that:
- 7.9.1 no staff may download software, programmes, and or applications to the device;
 - 7.9.2 no staff may use any other applications other than those authorised by and enabled on the device by the Owner;
 - 7.9.3 no staff may plug in and use any USB stick or other memory device with the Tecknuovo device;
 - 7.9.4 no staff may change or amend any login credentials or passwords provided by the Owner for the Tecknuovo device or for any IT systems to be accessed through the Tecknuovo device;
 - 7.9.5 staff may only access a customised browser which allows only whitelisted websites to be accessed and blocking all other websites;
 - 7.9.6 access to the internet is conducted via a corporate VPN; and
 - 7.9.7 all data usage and activity on the device can be managed and tracked remotely by the Owner.
- 7.10 The Supplier is required to inspect and test the Tecknuovo device on delivery and will notify Tecknuovo immediately if any Tecknuovo device does not reflect the configuration and customisation referred to in clause 7.9 above.
- 7.11 The Supplier shall ensure that neither it nor any staff seek to hack, amend, or otherwise tamper with any configuration or customisation of the Tecknuovo device or any passwords and/or log in details provided to the Supplier or any of its staff by the Owner to access the Tecknuovo device and or access to IT systems required.
- 7.12 The Supplier shall ensure that all staff who will use the Tecknuovo device in the provision of the services during any statement of work attends any induction and or training required by Tecknuovo for the correct operation of the Tecknuovo device including training on any IT systems to be accessed by staff through the Tecknuovo device. The Supplier shall bear the cost of any such induction and/or training required by Tecknuovo.
- 7.13 The Supplier agrees, during the term of any statement of work and thereafter until the Tecknuovo device is returned to the Owner, that it shall:
- 7.13.1 only utilise the Tecknuovo device in a secure area and shall keep the Tecknuovo device stored and secured overnight in the Supplier's offices;
 - 7.13.2 keep the Tecknuovo device in its possession and control and ensure that it is kept secure against loss, damage and theft (ensuring that such Tecknuovo device is stored in a locked cabinet or safe when not in use as a minimum);

- 7.13.3 operate the Tecknuovo device in a proper, safe and prudent manner in accordance with any operating instructions issued for it and for the purpose for which it was designed, and ensure that the Tecknuovo device is operated with all due care and attention and used by properly skilled and trained personnel in accordance with the Owner's relevant instructions;
 - 7.13.4 keep the Tecknuovo device in good working order, fair wear and tear excepted;
 - 7.13.5 not hold itself out as owner of the Tecknuovo device, nor shall it, charge, encumber, sell, let, lease, hire or otherwise dispose of, part with, or abandon the Tecknuovo device, nor shall it permit or suffer the creation of any lien or distress over the Tecknuovo device;
 - 7.13.6 not assign or transfers any of its rights or obligations in respect of the loan of such Tecknuovo device under this policy;
 - 7.13.7 ensure that any identification marks, labels or signs on or fixed to the Tecknuovo device are not removed, defaced, amended, obscured or otherwise subjected to interference, including those which identify the Tecknuovo device as belonging to the Owner;
 - 7.13.8 permit the Owner, Tecknuovo, and their respective employees and agents access to the Tecknuovo device and the Supplier's offices in which it is held for the purpose of inspecting, repairing, servicing and replacing the Tecknuovo device; and
 - 7.13.9 ensure that the Tecknuovo device is returned in the same condition that it was supplied in (fair wear and tear excepted).
- 7.14 If the Tecknuovo device suffers a breakdown the Supplier must immediately stop use of the Tecknuovo device, disconnect the Tecknuovo device from the power source (where appropriate), and notify Tecknuovo immediately of such breakdown.
- 7.15 The Supplier must not undertake or permit any repair work on the Tecknuovo device without the prior express written consent of Tecknuovo.
- 7.16 Subject to any express agreement to the contrary, all repair work shall be carried out by the Owner or his employees or agents and shall be carried out at the earliest mutually convenient opportunity.
- 7.17 Where the breakdown is caused by the negligence of the Supplier or by the misuse of the Tecknuovo device, the cost of repair or replacement of the Tecknuovo device shall be borne by the Supplier. Where the breakdown is caused by fair wear and tear or by a fault in the Tecknuovo device the cost of repair shall be borne by the Owner.
- 7.18 Should any Tecknuovo device be lost or stolen whilst in the possession of or under the control of the Supplier, the Supplier must notify Tecknuovo immediately of such loss or theft. In the case of theft, the Supplier shall ensure that it reports the theft to the police and obtaining a crime reference number, to be provided to Tecknuovo. The Supplier remains responsible for the full replacement cost of any Tecknuovo device lost or stolen whilst in its possession and or under its control.

8 Acceptable use of devices

- 8.1 Tecknuovo defines acceptable business use as activities that directly support the provision of the Supplier's services to Tecknuovo under a statement of work.
- 8.2 The Supplier shall ensure that the devices are blocked from accessing certain websites that Tecknuovo considers inappropriate while connected to any IT network.
- 8.3 The Supplier shall not and shall ensure that its staff do not access any IT network or IT system remotely from outside of the United Kingdom, even if for acceptable business use, unless with the prior written consent of Tecknuovo.
- 8.4 The Supplier shall ensure that its staff do not access any IT network or IT system:
- 8.4.1 from any site other than a secure area;
 - 8.4.2 from any public network (whether unsecured or purported to be secure);
 - 8.4.3 from any public place (irrespective of whether any network utilised is secure);
- unless with the prior written consent of Tecknuovo.
- 8.5 The Supplier shall where at all possible ensure that its staff utilise a wired network from the Supplier's offices for the provision of services under a statement of work. If staff are required to utilise a wireless network from the Supplier's office, the Supplier shall use all reasonable endeavours to ensure that the security of such wireless network is enhanced and and/or maintained by ensuring the following steps have been taken:
- 8.5.1 the password of the wireless router have been changed from their default and the password is strong and unique (recommended this be at least 20 characters long and include numbers, letters, symbols, and mix of lower/upper case letters);
 - 8.5.2 the SSID of the wireless router (i.e. network name) should be changed (where possible) and/or hidden;
 - 8.5.3 the network administrator password for network settings should be strong and unique;
 - 8.5.4 use stronger encryption e.g. WPA2 security or further enhanced security protocol (e.g. WPA3);
 - 8.5.5 maintain and update your wireless router software; and
 - 8.5.6 use a virtual private network (VPN).
- 8.6 The Supplier shall use its best endeavours to ensure that all supplier devices comply with the following to prevent unauthorised access to such devices in accordance with this policy:
- 8.6.1 automatic connectivity to wi-fi networks is switched off when devices are not in a secure area;
 - 8.6.2 bluetooth connectivity is switched off when bluetooth ancillary devices are not connected and/or supplier devices are not in a secure area.

- 8.7 The camera and/or video capabilities of any supplier device must be disabled while the Supplier and its staff are delivering services on-site at Tecknuovo premises or any customer premises unless with the prior written consent of Tecknuovo.
- 8.8 The Supplier shall ensure that any supplier device is not to be used at any time to:
- 8.8.1 engage in any activity that constitutes a breach of any of Tecknuovo's policies;
 - 8.8.2 store or transmit illicit materials;
 - 8.8.3 store or transmit proprietary information;
 - 8.8.4 harass, bully or unlawfully discriminate against others;
 - 8.8.5 defame or criticise Tecknuovo or its affiliates, customers, clients, suppliers, vendors and other stakeholders;
or
 - 8.8.6 breach any other laws or ethical standards.
- 8.9 The Supplier shall ensure that its staff use supplier devices to access IT systems pursuant to the requirements of a statement of work.

9 Security

- 9.1 In order to prevent unauthorised access, Suppliers must ensure the supplier devices are password or PIN protected using the features of the device. A strong password is required to access any IT network.
- 9.2 Chosen passwords must comply with Tecknuovo's password policy, which requires that you comply with the recommended standard set by Cyber Essentials, <https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-2-1.pdf>.
- 9.3 The device must lock itself with a password or PIN if idle for five minutes.
- 9.4 Suppliers must take all other reasonable efforts to secure their devices whether or not it is in use and whether or not it is being carried by any member of their staff. This includes, but is not limited to, the use of encryption and an enforced prohibition on the use of such supplier devices by anyone other than the Supplier's staff.
- 9.5 Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing any IT network.
- 9.6 Tecknuovo may from time-to-time issue details of types of devices that are not permitted to connect to any IT network, and/or to access Tecknuovo information (see paragraph 6 (Approved devices) above).
- 9.7 Any devices belonging to Supplier staff that are for personal use only should not be allowed to be utilised for the provision of the services or otherwise allowed to connect to any IT network or IT system.
- 9.8 Supplier staff access to Tecknuovo information on any IT system shall be limited based on user profiles defined by Tecknuovo and will be automatically enforced.

9.9 The Supplier shall ensure that data on its supplier devices may be remotely erased by the Supplier if required by Tecknuovo below if:

- 9.9.1 there is a data breach or potential data breach involving Tecknuovo information relevant to supplier device;
- 9.9.2 a device is lost or stolen;
- 9.9.3 a member of staff's password is lost or stolen;
- 9.9.4 any staff utilised on any Tecknuovo project is suspended from work or placed on garden leave by the Supplier in accordance with their employment contract with the Supplier;
- 9.9.5 the Supplier ceases to deliver services for Tecknuovo and you have not complied with your relevant obligations under paragraph 19 (Staff departure) below; and
- 9.9.6 Tecknuovo or its customer detects a virus, malware or other destructive program or code relevant to a supplier device.

10 Tecknuovo responsibilities

10.1 As a controller, Tecknuovo is responsible for ensuring that all processing of personal information which is under its control remains compliant with the Data Protection Act 2018, as amended from time to time, and the UK GDPR together (the **Data Protection Legislation**). In particular, Tecknuovo must:

- 10.1.1 use technical or organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- 10.1.2 implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into Tecknuovo's data processing activities; and
- 10.1.3 be able to demonstrate that it has used or implemented such measures.

11 Accessing and using Tecknuovo information

11.1 You are permitted to connect to or access only to IT systems from supplier device which Tecknuovo authorises (and whether or not owned or leased by Tecknuovo and which may include the IT systems of its customers that Tecknuovo has been authorised to access) and which may include but not be limited to the following:

- 11.1.1 Email;
- 11.1.2 cloud-based productivity suites
- 11.1.3 cloud-based document management and storage system;
- 11.1.4 Supplier online portal;
- 11.1.5 Tecknuovo online timesheet portal;
- 11.1.6 calendars;

- 11.2 The Supplier shall and shall ensure its staff only use Tecknuovo information to provide services to us and not for any other purpose.
- 11.3 You must only use Tecknuovo information with the security protocols herein and any additional security protocols that Tecknuovo may require the Supplier to comply with, with respect to the use of Tecknuovo information.
- 11.4 Tecknuovo information remains its property at all times, no matter what format it is in, where it is stored or how it is accessed.
- 11.5 The Supplier agrees to give Tecknuovo access to any Tecknuovo information on supplier device immediately on its reasonable request. In this context, 'access' includes Tecknuovo being permitted to access, make copies of, recover or delete files (including all copies of files) containing Tecknuovo information from supplier device.

12 Regulatory reasons and audit

- 12.1 From time-to-time Tecknuovo may need to access and/or audit supplier device (and the information and applications on it), in order to pursue the following legitimate business purposes (together the regulatory reasons):
- 12.1.1 to verify your compliance with this and other Tecknuovo policies;
 - 12.1.2 to ensure that Tecknuovo complies with its obligations to its regulators, the courts and other relevant official bodies (regulators);
 - 12.1.3 to demonstrate to regulators that Tecknuovo has been complying with its legal and regulatory obligations; and
 - 12.1.4 to cooperate with any investigations, proceedings or other requests for information by the regulators.
- 12.2 In using the supplier device as envisaged by the provisions of this policy, the Supplier authorises Tecknuovo (or its authorised agents or representatives, such as auditors or regulators) to access and/or audit supplier device for regulatory reasons, as Tecknuovo reasonably require from time to time. You agree to co-operate with and facilitate any such access and/or audit.
- 12.3 Tecknuovo appreciates that supplier device will contain both Tecknuovo information and your personal information.
- 12.4 If the Supplier complies with the separation protocols and the security protocols, any intrusiveness or inconvenience to it of Tecknuovo accessing and/or auditing supplier device is likely to be minimised.

13 Services Tecknuovo provides

Tecknuovo reserve the right to (temporarily or permanently) disconnect, disable, restrict use of or modify at any time any services that it provides and that the Supplier accesses via supplier device at any time, for any reason and without prior notice.

14 Your responsibilities concerning supplier device

- 14.1 You are at all times solely responsible for:

- 14.1.1 purchasing supplier device, paying all device and carrier service costs, bills and tariffs for supplier device, including but not limited to voice and data usage charges;
 - 14.1.2 repairs to and maintenance of supplier device and the associated costs, including costs required to replace supplier device;
 - 14.1.3 running backups of your own data on supplier device daily and weekly;
 - 14.1.4 ensuring periodic system/security upgrades are installed without delay when notified of their availability; and
 - 14.1.5 *[insert any other specific responsibilities]*.
- 14.2 You agree that you use supplier device at your own risk and that Tecknuovo will not be responsible for any losses, damages or liability arising out of its use (to the extent permitted under applicable law).
- 14.3 Tecknuovo recommends that the Supplier insures all supplier devices (eg as part of its business insurance policy).

15 Data privacy standard

- 15.1 You are referred to Tecknuovo's privacy notice and/or data protection policy, which establish Tecknuovo's data privacy standard. You are required to act in a manner consistent with that standard during the statement of work and also in the operation of any device under this policy.
- 15.2 The Supplier is required to enter into a data processing agreement with Tecknuovo as a sub-processor in respect of any Tecknuovo Information which is classified as personal data (for the purposes of the Data Protection Legislation). You agree that you will comply with your obligations as a processor under Data Protection legislation and pursuant to any data processing agreement.
- 15.3 You may only transfer personal information outside the United Kingdom with the prior and express written consent of Tecknuovo.

16 Risks you accept

- 16.1 You acknowledge that there are specific risks associated with you using supplier device for work purposes in accordance with this policy. These risks include the threat of viruses, malware and other software and/or hardware failures or programming, operating system or other errors that may result in loss of data (yours and/or Tecknuovo information) or supplier device not working properly or at all.
- 16.2 However, as the user of supplier device, you agree to accept and assume full liability for these risks (except for any liability that we cannot by law exclude or limit).

17 Theft or loss of device

- 17.1 If any device is lost or stolen, you must inform Tecknuovo immediately and no later than close of business on the relevant day.

17.2 The quicker you inform Tecknuovo of this and cooperate by providing such information and assistance as Tecknuovo request, the more effectively Tecknuovo will be able to assess and contain any potential data security breach risk and any other relevant risks. This will in turn impact the level of our response and the action Tecknuovo needs to take.

18 Data security breach

18.1 If you become aware of a breach of security or believe that any device may have been accessed by an unauthorised person or otherwise compromised, you must inform Tecknuovo as soon as possible and in any event by no later than close of business on the relevant day.

18.2 Both you and Tecknuovo have legal obligations under Data Protection Legislation. The quicker you inform Tecknuovo of any breach of security and cooperate by providing such information and assistance as Tecknuovo requests, the more effectively Tecknuovo will be able to assess and contain any potential data security breach risk and any other relevant risks. This will in turn impact the level of our response and the action Tecknuovo needs to take.

19 Termination of statement of work

19.1 Upon the termination of any statement of work (regardless of the reason for termination):

19.1.1 the Supplier's access to any IT system, its applications and all Tecknuovo information will cease;

19.1.2 Tecknuovo device will be delivered up to Tecknuovo; and

19.1.3 all Tecknuovo information on supplier device will be delivered to Tecknuovo and the supplier device will be wiped (permanently deleted) upon the written instruction of Tecknuovo.

19.2 You are reminded that the Supplier's obligations to keep Tecknuovo information confidential continue even after the termination of any statement of work.

19.3 If Tecknuovo request, you will sign a written declaration confirming supplier device contains no Tecknuovo information and/or allow Tecknuovo to inspect supplier device to confirm supplier device contains no Tecknuovo information. The Supplier will provide all necessary co-operation and assistance to the Tecknuovo in relation to this process.

20 Failure to comply with this policy

20.1 Failure to comply with this policy may result in the termination of any statement of work, including, where appropriate, revocation of access to the IT systems, and criminal prosecution in accordance with local laws. As well as any specific rights Tecknuovo has in this policy that apply where the Supplier breaches particular provisions of this policy, the Supplier's breach of its obligations under this policy will constitute a breach of its contract with Tecknuovo and Tecknuovo may exercise its rights under that contract. If you have reasonable grounds to suspect that someone else is in breach of this policy, you must inform Tecknuovo immediately.

APPENDIX 1
APPROVED DEVICES LIST

APPENDIX 2 SEPARATION PROTOCOLS

You shall comply with the following protocols for the purpose of separating Tecknuovo information from your data on supplier device:

organise files within supplier device into specifically designated folders that clearly differentiate between information that is Tecknuovo information and information that is personal information;

label work-related and personal correspondence using distinctive identifiers in the subject line (ie 'PERSONAL...' for personal emails;