-
-
-
-

-
-
-
-
-

10.

10.1 You must not use public Wi-Fi to connect to the internet on a WAT device. For example, if you are working in a public space then you will either need to work offline or use 3G / 4G.

10.2 All use of the Internet is governed by a legal agreement with our Internet Service Provider (ISP) in addition to the guidelines here. If you use a personal computer at home for work

- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the trust's IT facilities.
- Causing intentional damage to IT facilities.
- Removing, deleting, or disposing of IT equipment, systems, programmes or information without permission.
- Accessing, modifying, or sharing data (including Personal Data) to which a user is not required to have access.
- Promoting a private business, unless that business is directly related to the trust.
- Using websites or mechanisms to bypass the trust's filtering mechanisms.
- Intentionally damage, disable, or otherwise harm the operation of systems.
- Excessive downloading of material from the Internet.

13.2 This is not an exhaustive list. and there may be other examples that may warrant further investigation and consideration for disciplinary action if appropriate.

13.3 WAT's Child Protection and Safeguarding and E-Safety policies contain additional information relating to safeguarding and online safety with acceptable use agreements, that should also be read in conjunction with this policy.

13.4 In exceptional circumstances only, where the use of Trust IT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the executive/ headteacher's discretion only.

14.

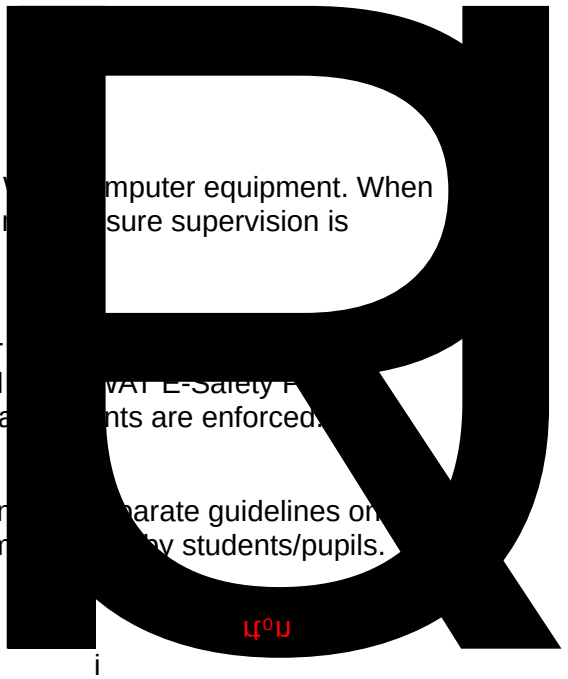
14.1 All users should set strong passwords for their accounts and keep these passwords secure. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

- . If communicating with a student/pupil via email, the WAT account must be used.

  . Caution should be exercised when using blind copying (bcc) emails to avoid entering email addresses in the cc field rather than the bcc.
- For example, when sending details of a safeguarding in

ha

- If travelling by public transport, the documents must be kept with you at all times, and they should not be stored in luggage racks.
- If travelling by car, documents must be kept out of plain sight. Please be aware that possessions left on car seats are vulnerable to theft when vehicles are stationary e.g., at traffic lights.
- If there is a choice between leaving documents in a vehicle and taking them with you (e.g., to a meeting) then you should usually take them with you and keep them on your person in a locked case. The risks of this situation should be reduced by only having the minimum amount of Personal Data with you.



20.1 Pupils/students must be supervised at all times when using mputer equipment. When arranging use of computer facilities for pupils/students, you sure supervision is available.

20.2 Academies need to ensure that there is an Acceptable User pupils/students and implement the requirements as outlined VAT E-Safety P Supervising staff are responsible for ensuring that these arra nts are enforced.

20.3 Supervising staff must ensure they have read and understar parate guidelines on E-safety, which pertains to the child protection issues of com by students/pupils.

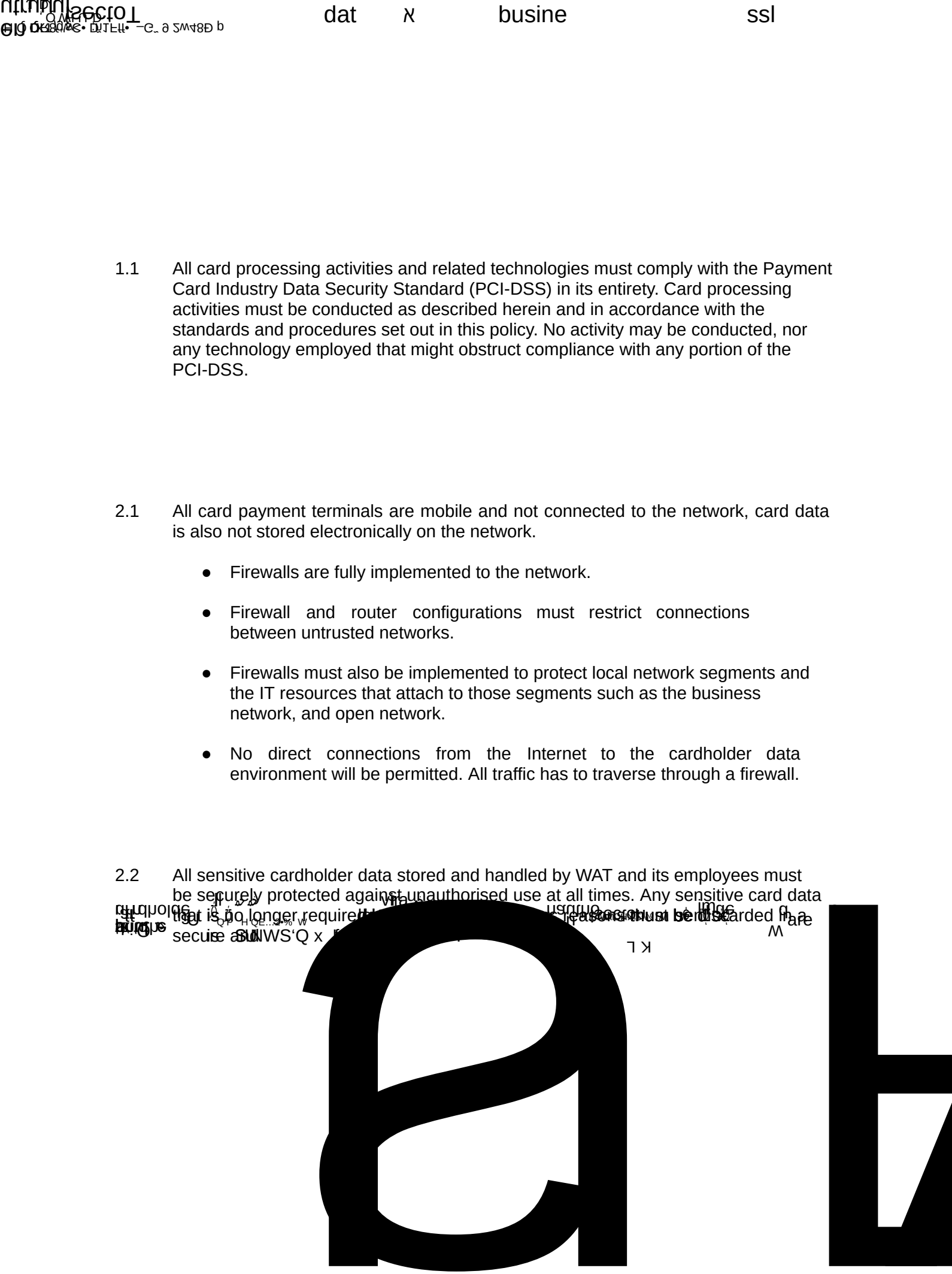
nts
sion
stu

1.1 All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures set out in this policy. No activity may be conducted, nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

2.1 All card payment terminals are mobile and not connected to the network, card data is also not stored electronically on the network.

- Firewalls are fully implemented to the network.
- Firewall and router configurations must restrict connections between untrusted networks.
- Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- No direct connections from the Internet to the cardholder data environment will be permitted. All traffic has to traverse through a firewall.

2.2 All sensitive cardholder data stored and handled by WAT and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required



system as well as from the trash bin. No one should forward any email, which they suspect may contain viruses.

- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices receive training and are restricted to only those necessary for business purposes.
- Any 3rd party maintenance, updates or device replacement is arranged centrally by the finance manager only and the validity of any work is verified prior to work being carried out.
- Terminals are kept locked in either a secure room or safe outside of business hours, during business hours all terminals are in the constant presence of an employee and not left unattended.
- All receipts are kept securely during day-to day operations and then transferred to the finance office for secure storage.