FJSS GROUP

COMPUTER &DEVICE USAGE POLICY

COMPUTER, LAPTOP, IPAD, AND OTHER IT DEVICES (ORGANISATION DEVICES) POLICY & PROCEDURE

INTRODUCTION

1.1 Any laptop, computer, iPad, tablet, or mobile device or other (with internet/email facilities) (hereafter referred to as a computer or organisation device) issued to you by FJSS Group (hereafter referred to as the Organisation) will remain, at all, times the property of the Organisation.

ABOUT THIS POLICY

2.2 This policy is the guiding document for custody and usage of all electronic devices and gadgets of the organisation. Any violation of this policy that results in the damage, significant changes of settings as well as the unauthorised erasure and deletion of files, documents, photographs, and all other materials stored on the any issued device that compromises the integrity and operations of the organisation will lead legal action or criminal prosecution at the instigation of the organisation.

2.3 This policy applies to all members of staff and volunteers who are issued with a computer or electronic device, by the organisation and it is the responsibility of all staff and volunteers issued with the computer or electronic device to comply with this policy

2.4 It must be clearly understood that the issue of computers and devices to staff and volunteers is for the purpose of improving the Organisation's workflow and communication systems and is not intended for personal or commercial use.

2.5 Accessing any work-related activities with the exception, of, emails on devices not issued to you by the Organisation is not permitted unless you have previously obtained written permission from a manager. If such permission is obtained key locks and/or passwords must be in place as well as individuals adhering to this policy and all others relating to the work of the organisation.

MANAGEMENT RESPONSIBILITIES

3.1 All computers and devices issued must be authorised by the IT department of the Organisation.

3.2 A register of all computers and devices will be maintained and updated as and when required.

3.3 The Organisation will monitor the usage of computers and devices to investigate any discrepancies that may be identified at any time.

STAFF AND VOLUNTEER RESPONSIBILITIES

4.1 Every member of staff and volunteer will be asked to sign this policy to confirm receipt of their computer, and to acknowledge that they have read, understood, and will comply with the requirements of this policy.

4.2 Members of staff and volunteers are required to keep the computer or device issued to them fully charged so that it can be used for an entire working day.

4.3 Staff or volunteers leaving the Organisation must return their computer or device to the IT department at Justice House beforehand. The member of staff or volunteer's line manager is responsible for ensuring that this is done.

4.4 Failure to return the computer or device in good working order, when requested to do so by the Organisation will incur a penalty charge of 50% of the current value of the computer or device which will be immediately requested to be paid by the member of staff or volunteer or where applicable and involves a paid member of staff, this will be deducted from the staff member's final salary.

4.5 If for any reason an employee is requested to return their computer or device to the Office by the IT department, they must do so immediately. Failure to return the computer in good working order, when requested to do so by the Organisation will incur a penalty charge equivalent to value of repairs or replacement required as necessary, which will be effected similarly as in clause 3.4 above.

SECURITY

5.1 Members of staff and volunteers issued with a computer or device must always ensure the security of the computer or device, and this means in work and outside of work.

5.2 Members of staff and volunteers are responsible, when away from their work setting to ensure that their issued computer or device is protected against loss or theft.

5.3 The Organisation instructs all members of staff and volunteers to adhere to the following:

- Secure the computer at home as if it is a personal possession ensuring it is covered on their home contents insurance
- Computers must not be left in unattended vehicles
- While in the office, store the computer and associated equipment with due care
- Keep food and drink away from the computer.
- Always ensure hands are clean and free of transferrable fat/oils that might damage the com puter or device screen and keyboard
- When travelling by car, computers or devices must be stored securely and out of sight.
- When travelling, computers and devices should not be left unattended in public places.
- It is the responsibility of all staff members and volunteers to ensure that all laptops and tablets are password protected and not to disclose this to anyone.

STOLEN, LOST OR DAMAGED COMPUTERS

6.1 It is the staff member or volunteer's responsibility to take good care of the computer or device and take all reasonable precautions to ensure that the computer or device is not damaged, lost or stolen

6.2 In the event that the computer or device is stolen, the employee will be expected to immediately report the theft to the police and obtain a crime reference number – within 24 hours. In addition to this they must also immediately inform the IT department.

6.3 In the event that a computer is lost, this must also immediately be reported to the member of staff's line manager and a short report should be written on how the computer was damaged.

6.4 In the event that a computer is damaged, this must also immediately be reported to the IT department and a short report should be written on how the computer was damaged.

USAGES

7.1 Computers and devices which include email usage, are for business use only and not for personal use.

7.2 Usage of computers/emails will be monitored and any employee who is found to be using their computer for personal use will be liable to disciplinary action.

7.3 Misuse of the Internet and E-mail is regarded as a serious breach of this policy as well as our Data Protection and Acceptable Use policies as well as GDPR compliance.

7.4 If you view, access, download or distribute pornographic and / or other offensive or criminal material from the Internet or send, view, or distribute damaging or offensive or criminal e-mails this will be regarded as gross misconduct which will result in a summary dismissal.

7.5 Unauthorised or unlicensed software must not be downloaded or installed on computers or devices.

7.6 Ensure the computer or device is not used by any unauthorised persons

7.7 Usage of iPads within the Childcare settings to take photos are only allowed in the event of the settings camera being unavailable.

7.8 Photo's that are taken for observations, internal noticeboards and child development purposes must have the parents' permission and must be printed then deleted from the device.

7.9 Storage of photos in the Cloud is strictly prohibited and failure to adhere to this policy may result in disciplinary action.

WORKING OUTSIDE OF THE OFFICE

8.1 All mobile devices (including, but not limited to, laptops, tablets, and mobile telephones) provided by the Organisation should always be transported securely and handled with care.

8.2 Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes or Organisation's premises.

8.3 If any such mobile device is to be left in a vehicle it must be stored out of sight i.e., locked in the boot or glove compartment depending on size.

8.4 Where possible the transport of data in paper form containing personal information should be limited or avoided.

8.5 The use of an encrypted USB is acceptable if there are no other alternatives. Ideally documents should be scanned and used on-line with the exception, of where they require signatures.

8.6 Personal data should not be left in cars.

8.7 It should be stored securely and returned to the office at the earliest opportunity.

8.8 If you need to log on to your laptop when out of the office, please be cautious when you first access a new network. You may see a terms of use banner, or you may be asked to enter identi-

8.9 Read the text and be sure to understand how that information might be used. In locations with many Wi-Fi networks available, make sure you are connecting to the right one. Avoid where possible, falling victim to a rogue hotspot, and do not use an unsecured network if you have access to a password-protected option.

8.10 Once you are online, only submit sensitive information on secure websites, with URLs that start with 'https' instead of 'http' (see below). You will also see a padlock for secure sites.

8.11 This means that the site is encrypted, and your data has a greater degree of safety; 'https' sites are not immune to hackers, but an unsecured site that should be secure will have potential risks and should not be used.

8.12 Sensitive browsing (like online banking or shopping) should be avoided on shared networks entirely as should the accessing of our hosted on-line systems including Outlook.

8.13 It is imperative that you download app and operating system (Windows) updates promptly.

8.14 Updates often patch up software vulnerabilities and keep everything running smoothly and securely. We do have reliable anti-virus/anti-malware programs monitoring the health and security of our systems however it is essential that you closedown your PC or Laptop completely on a regular basis to allow these to run.

INTELLECTUAL PROPERTY OWNERSHIP

The information contained in files, emails, or any other forma, held on the computer, laptop, tablet or any such electronic device as issued to the member of the team of the team remains the sole property of FJSS Group. Any tempering with, deleting, resetting of devices, formatting, editing, downloading, and transferring of such information onto third party devices without the express permission and knowledge of FJSS Group will be viewed as criminal and the member concerned will be prosecuted and or sued for any loss, damage, and breach of client confidential protocols.

DECLARATION

STAFF/VOLUNTEER
I hereby agree to abide by the terms, conditions and procedures as stated in this policy.

Full Name: _____

Position: _____

Signature: _____

Date: _____/_____/_____

FOR AND ON BEHALF OF FJSS GROUP
I hereby agree to abide by the terms, conditions and procedures as stated in the Computer, Laptop, and other Devices Policy & Procedure for FJSS Group

Full Name: _____

Position:_____ Signature: _____

FJSS GroupJustice House 24-26 Main Street West Calder West Lothian EH55 8DR
administration@fjssgroup.org +44 131 285 1013 www.fjssgroup.org