IT & Communication Policy

Purpose:

The purpose of this policy is to ensure all staff and volunteers are provided with guidance on using PIP's ICT facilities responsibly.

Contents:

Appendix:

Related Documents:

Data Protection
Finance Policy

1. Policy Principles:

All PIP ICT facilities and information resources remain the property of PIP and not particular individuals.

By following this policy we will help ensure ICT facilities are used:

- Legally
- Securely
- Without undermining PIP
- Effectively
- In spirit of co-operation, trust and consideration for others.

This policy and good practice guidelines relate to all information and communication technology facilities and services provided by PIP. All staff are expected to adhere to it. Non-compliance could constitute a serious disciplinary matter.

Data includes all files or media produced and stored on any of PIP's facilities and emails sent or received and stored in mailboxes on the server, weather business or personal in nature.

ICT equipment includes, but not exclusively, all computers, tablets, laptops, mobile phones, telephones, cameras, storage devices, printers, or any other electronic devices or associated equipment.

It is assumed that staff and volunteers will act responsibly in the use of ICT systems and on that basis the organisation does not proactively monitor email, internet or telephone usage, although this facility does exist if required and the Management/Board reserves the right to monitor any aspects of its telephone or computer system.

The internet and email are provided to employees as part of their equipment to work and are an integral and vital part of the organisations business, however, there are risks involved into the use of the facilities and inappropriate use of email could damage the business and reputation of PIP. It is therefore essential that employees read this policy and [procedures and make themselves aware of the potential liabilities involved in using the internet and email.

Examples of risks include:

- Claims of defamation (of other people and organisations)
- Breach or loss of confidential data (see Data protection policy)
- Breach of copyright or licensing laws
- Harassment and discrimination
- Agreeing to contract by mistake]
- The introduction of viruses to the network.

2. Use of Equipment

Certain employees, if approved by the Board, may be provided with use of a laptop, tablet or mobile phone when working away from the office. These business assets are provided for sole use of employee and only in connection with their employment with PIP. Use of these assets for personal and private use is limited as outlined in this policy.

3. Theft or Damage to Equipment

Laptop, tablet and mobile phones are cover by PIP's insurance policy. However, if equipment is left unattended in a vehicle this will not be covered or under employees car insurance if they are stolen. Users should inform the police and PIP as soon as possible if any ICT equipment in their possession is stolen. Damage to, or loss must be reported immediatley so that replacements or repair can be made efficiently and cost effectively.

4. Copyright

Take care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside of these agreements is illegal and may result in criminal charges.

Copyright applies to all text, pictures, sound or video, including those sent by email or internet. File containing such copyright protected material should not be forwarded or transmitted to third parties with the permission of the author. Software licensing and compliancy is very stringent and heavy fines can be imposed if an organisation is found not to be compliant.

5. Security and storage of data

Do not attempt to gain unauthorised access to information or facilities. The computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PC's) or to modify its contents. If you don't have access to information recourses you feel you need, contact your line Manager.

All computers, laptop and tablet should be password protected to prevent access by external agents. The password will be used will be issued by your line Manager or IT support company and should not be changed without consultation. Central records of passwords are held by the Manager and Administrator. Passwords should be changed regularly.

Do not disclose personal system passwords or other security details of other staff, volunteers or external agents except when required to enable IT support. Disclosure of passwords may be required in some circumstances but only

allowed if sanctioned by a Manager or Trustee. Never store passwords on your laptop, tablet or desktop.

Unattended PC's/laptops must be locked or logged off. If you leave your PC unattended without logging off, you are responsible for any misuse of it while you're away. The organisation will assume in the first instance that any material from or via you computer was generated or passed on by you. When working outside of the office particular care must be taken to ensure there is no unauthorised access to data.

Mobile phones must have the auto lock and password facility active. When travelling always keep your equipment with you unless there is a more secure option and do not leave unattended in a vehicle.

Any security incidents or breaches should be reported immediately to your Line Manager. Always check removable storage devices for viruses prior to use.

6. Data storage and Back-up

Staff/Volunteers should comply with the procedures set down in this policy and the PIP Data Protection Policy concerning data storage, locations, data responsibility, data security and back up.

Server based storage is provided to all staff and volunteers via a mapped drive to the PIP data folder. All PIP data including photos should be stored in this location for security and protection.

Do no copy files which are accessible centrally into your personal drive unless you have a good reason since this used up disc space.

The use of removable storage devices or personal laptops/tablets/desktops or any other storage media not falling within the sever security to download or store any PIP confidential or sensitive material including client information/records/case notes and supervision notes is strictly prohibited.

Personal data should not be stored on PIP equipment and this includes personal photographs, letters, documents and any other matter which does not directly relate to the employees work with PIP.

A daily nightly back up is automated using "Google Drive" and all information held within the PIP data file is backed up. It is then synchronised with the cloud service providing off site back up and on site a back up is also made onto an external hard drive. Systems are set up on the desktop of the Office Administrator's work station.

7. Network security

Individuals are responsible for safeguarding their network accounts and mailboxes and should inform their Manager is they think their computer or mailbox has been compromised in anyway.

When using the shared drive members should respect other users and should not delete or amend documents without the agreement of the author of the document or line manager concerned.

8. Electronic Monitoring

No private information personal to the user is to be stored on the computers belonging to PIP. Any information that is stored including files, emails notes etc may be accessed and inspected by Manager and member of the ICT support.

Any equipment being used by any member of staff must be made available for inspection and/or returned to Pip office at any time when requested by a Manager or ICT support.

Emails maybe monitored and could be inspected or made available as evidence to any body or person who may legally require access to this information.

9. Electronic Mail and internet

Access to email and internet is provided for business purposes only. All staff members and trustees will be provided with an email mailbox. This mailbox is also available via Outlook Web Access and access is provided to some staff via their mobile phone.

Occasional but infrequent use of email and internet for personal purposes is acceptable but should be in your own time and should not interfere with your work. Excessive private use may lead to disciplinary actions.

You are a representative of PIP when you are on the internet and using email. Therefore make sure your actions are in the interest (and spirit) of PIP also avoid trading insults with other people with whom you disagree.

The creation, download and dissemination of any obscene, pornographic or blasphemous material by staff or volunteers are strictly prohibited.

Staff and volunteers must not use their personal email accounts to communicate with clients or in connection with PIP business or subscribe to chat rooms,

messaging services or other on-line subscriptions on behalf of the organisation unless it has been authorised by your Line Manager.

10. Using Electronic Mail

Email has many of the same characteristics as letters and faxed. It is as permanent and indestructible as writing. Email which you may have deleted can be retrieved from hard disk and may be used in court or tribunal proceedings.

Transmission of sensitive or confidential data by email:
Where it has been agreed that confidential/sensitive information may be sent electronically this must be sent using the Egress Switch Encrypted Email Service.

When should you use encrypted email?
Whenever you need to send an email that contains personal, sensitive or confidential information you should use the encrypted email option available to most staff. Primarily this will be in relation to client data but it may also apply to other personal information you may need to send. If in any doubt then choose to encrypt the message.

Do not put any personal details or names in the subject line and check you have the correct data consent permissions and that you are only sending details that are necessary.

Please refer to appendix 1 for the guidelines for sending encrypted emails.

Email Signature:
Emails sent from the organisations mailboxes/sever must include the PIP "signature". This template is provided to all staff at induction who may only edit the name and job title. All other details including company status and Number, Charity Reg No, registered address and disclaimer will remain uniformed for all staff and trustees.

Use of group emails and Distribution lists:
Group mailings and large distributions will be sent by the Office Administrator or Manager.

Only send email to those it is meant for; don't broadcast unless absolutely necessary since this runs the risk of being disruptive. When circulating emails to people outside the organisation, consider using the blind carbon copy, i.e. the bcc option so that other external persons are not able to see the other recipients email addresses.

11. Use of telephone

The telephone system is used for the purposes of PIP business activities. Personal use of PIP telephones and mobiles is not permitted unless exceptional circumstances. Staff members should consult their Manager

12. Mobile Telephones

Mobile phones are supplied to some staff on a job need basis. Each mobile phone should have a registered user and that user will be responsible for the use and security of the telephone. The user must report the loss or damage to their phone to their Manager.

It is the individual staff member's responsibility to ensure that they are legally compliant when using their phone in particular when driving.

It is the responsibility of the employee to ensure their mobile is kept charged and switched on during their working hours particularly when working away from the office.

Staff should ensure that the auto lock facility is activated for security purposes. Staff's Personal email accounts should not be added to the PIP mobile phone.

Text messaging to clients must only be used for short non-essential messages i.e. confirming appointments but have regard to their preferred method of communication.

The camera facility must not be used to take images of people.

Staff should not use their personal phones or mobiles to communicate with clients.

13. Tablets

PIP Tablet may be used by some staff or volunteers on a job need basis or on loan where it is deemed appropriate to use for a particular PIP activity or event.

It is the responsibility of the employee to ensure it is kept charged and is kept safe without being left unattended.

Downloading of apps or personal data is strictly prohibited. It may only be used for PIP business and not personal use.

The camera facility must not be used to take images of people.

Each User must book the tablet out with the Manager or Administrator before removing from the office. A short explanation of use conditions and unlock code will be given.

14. PIP website and Social Media

www.pipcroydon.com. Overall responsibility of this site remains with the board of Trustees but the Manager is responsible for overseeing the operational aspect of the site and social media. Staff members should liaise with The Manager is they wish to amend or remove content.

Permission to access and update Facebook/Twitter is limited to authorised personnel only.

Staff should not communicate with clients using open social networking and instant messaging or share any personal information and should not request or respond to any information from a client other than that which might be appropriate as part of their professional role. All communication must be transparent and open to scrutiny.

15. Hardware and software

All workstation are installed with a default list of software. Additional software may be installed where this is appropriate to the particular service or individual role and would normally be identified on induction or supervision.

Any hardware or software purchases are to be agreed by the Trustees, please refer to our Finance Policy COP002.

The use of personal equipment on the organisations internal network is not permitted with prior authorisation by The Manager.

16. Use of IT facilities

As a general rule you should use the facilities during working hours solely for the purpose of work. Sending and receiving personal emails or browsing internet is permitted as long as it is done in own personal break times and conforms to the guidelines in this policy.

17. Care of equipment

Do not re-arrange how equipment is plugged in or move any equipment or accessories with first contacting to IT support Company. Do not place food or drink in close proximity to ICT equipment

18. Maintenance

PIP has an IT support agreement with a suitable provider to ensure that all ICT equipment is maintained to a high standard, that all equipment has the appropriate software and specifications and to advise where updates or modifications are required.

The IT support service will oversee routine system maintenance and ensure that system backs ups and Anti-virus are regularly monitored and updated.

Routine remote access maintenance takes place on Monday evenings at approximately 6pm. It is important that all staff leave PC power on but screen is switch off. Staff will not be able to access the system during this time.

If you experience any problems with your PC please speak to your Manager or contact our IT Support Company via support@digitalmedic.co.uk.

19. Training

All staff will be provided with the basic skills to operate Microsoft Office and familiarised with the organisations ICT procedures. Additional training needs will be monitored including any specific software required to fulfil their role and met as necessary. Requests for training should be done via their Line Manager as part of their supervision process. It is expected that staff will attend appropriate training wherever update of skills are necessary for carrying out their job.

This IT Policy was approved at a meeting of the Board of Trustees on:

Julie Newton-Smith **Chair of Trustees**	**Signed:**	**Date:** **Review: July 2018**

IT & Communication Policy

Appendix 1

GUIDANCE ON USING THE EGRESS SWITCH ENCRYPTED EMAIL SERVICE

Encryption is now available when using electronic mail for transmitting confidential or sensitive information. Encryption is an option which you need to select to ensure the email is encrypted.

WHERE TO FIND THE ENCRYPTION TAB
In Outlook when you select the New Email Tab – you will notice that there is a tab on the left hand side which has the egress switch logo.

When sending an email you should select the “unprotected” tab with a drop down arrow. This will allow you to choose whether you wish to send the email unprotected or to select the encrypted version with the padlock icon. If you do not use this tab the email will at present default to standard UNPROTECTED email.

If you choose ENCRYPTED this will encrypt both the message content and the attachments but **NOT** the subject line. Therefore you should **never** put a name or any personal details in the subject line.

There is a further tab with the Egress icon which is entitled” package restrictions”– these enables you to set a time period when the contents and attachments are accessible should you feel this is necessary.

WHO CAN ACCESS AN ENCRYPTED EMAIL:
Only the specific email address that you send the email to will be able to access an encrypted email that you generate. If the email is forwarded on by that person the new receiver will not be able to open the email without your permission.

HOW CAN I MANAGE ENCRYPTED EMAIL?
An audit of any encrypted email can be viewed from your Switch account which is accessed from the icon in the toolbar at the bottom right of your screen or by clicking on the Egress Switch Icon on your desktop and going to “my packages”

This will show you who the email has been sent to and will indicate whenever the email has been accessed.

“My Packages” also allows you to add or withdraw access to a particular email at anytime.

If an email has been sent inadvertently you should access “My Packages” and deny access as soon as possible.

Similarly if you want to allow an additional email address access – you can add the details after the email has been sent.

You will have control over the email at all stages. However please note that this does not prevent a user you have sent information to from saving a copy of the information and then transmitting this data independently.

WHEN SHOULD I USE ENCRYPTED EMAIL?
Whenever you need to send an email that contains personal, sensitive or confidential information you should use the encrypted email option.
Primarily this will be in relation to confidential client data but it may also apply to other personal information you may need to send. If in any doubt then choose to encrypt the message.

Do **NOT** put any personal details or names in the subject line. Check that you have the correct data consent permissions and that you are only sending details that are necessary

WHAT DOES THE PERSON RECEIVING ENCRYPTED EMAIL NEED TO DO?

Whenever an encrypted email is sent the recipient will receive a notification email that advises them that they have received an encrypted email from you and prompts them with a pop up box to sign into their Switch account to open the message. If it is the first time they have received an encrypted email from you it will prompt them with setting up an account. This is a one off step similar to the set up each of you has already experienced. It is free and only takes a few moments.

After this they will be able to enter their user name and password to open future emails.

The system will also enable them to reply to you using the same encrypted service.

GUIDANCE

There are also a number of easy to view guides and videos on the Switch Egress Website at http://www.egress.com/solutions-secure-email