Plymouth School of Creative Arts

make discover perform

Plymouth School of Creative Arts

Data Handling and Electronic Communications Policy

Date created: 13/03/13	Created by: M. Sweeney,	Review period: Annually
Reviewed: May 2018	By Digital Team	Next Review Due: May 2019

Contents

1. Introduction

1.1 Plymouth School of Creative Arts (PSCA) has a whole school data handling system designed to identify student potential and targets and then allow monitored intervention strategies to be put in place.

1.2 As electronic communications become faster, more powerful and easier to use there is also, sadly, an increased risk of damage being caused through inappropriate use. This document also sets out how PSCA seeks to ensure that its staff and students use electronic communications responsibly.

1.3 PSCA processes a substantial amount of confidential and personal data and information on private individuals, employees, service partners and its own operation. This information is vital for PSCA to fulfil its role properly. Therefore the risks to its confidentiality, integrity and availability must be identified, quantified and mitigated. Please refer to PSCA's Data Protection Policy which sets out how PSCA complies with its obligation under the General Data Protection Regulation (GDPR).

1.4 Personal data is any or all information relating to an identified, or identifiable, individual. This may include the individual's name (including initials), an identification number or an online identifier (such as a username). It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity (**Personal Data**).

1.5 Personal Data which is more sensitive and so needs more protection is classed as **Special Category of Data**. This can include information about an individual's racial or ethnic origin, their political opinions and their physical or mental health.

1.6 The Data Handling and Electronic Communications Policy applies to everyone who uses PSCA computer equipment, the PSCA computer network or telephone systems including;

- Students of PSCA;
- All employees of PSCA;
- Others given access to PSCA's computer systems or information including partners, suppliers and other third parties.

1.7 All users must abide by the policy set out in this document at all times. In addition, users must use systems responsibly, comply with PSCA requirements and operate within the law.

1.8 The policy applies to all equipment which facilitates electronic communications. This includes devices with computer-like functionality, which can manipulate information, and also to storage-only devices. These include, but are not restricted to;

- PCs and laptops
- Tablet PCs
- Electronic organisers

- Computer servers
- Digital cameras
- Scanners
- Telephones
- Mobile phones
- USB memory sticks
- CDs and DVDs
- External hard disks
- Network Connected Photocopiers
- Network connectivity devices e.g. modems and broadband devices
- Devices capable of wireless connectivity such as infrared and Bluetooth.

1.9 To be included in this policy a device does not have to be capable of manipulating the information it holds, because all electronically stored information is capable of (i) being inappropriately disclosed and (ii) carrying malicious codes which could disrupt the PSCA's computer network and systems.

1.10 This policy applies to all forms of data and information, which is owned by, administered or controlled by PSCA. This includes, but is not restricted to, text, still or moving images, maps, diagrams, video, audio, CCTV, music and sound recordings.

2. Risks of Electronic Communications

2.1 Misuse of PSCA's electronic communication facilities could expose both, PSCA and individuals to the risk of legal claims against them including claims of defamation, discrimination or harassment, breach of copyright or contract, breach of the duty of confidentiality. It could even include criminal prosecution if child or violent pornography, materials promoting terrorism, racial, religious or sexual hatred, unlicensed software or unlicensed music files such as MP3s on the computer network is discovered, and criminal prosecution or civil action following a breach of data protection legislation.

2.2 In addition, misuse of PSCA's facilities could prejudice the availability and security of PSCA computers, computer network and the information held on or accessed through the computer network.

2.3 Such security breaches could potentially damage the PSCA's reputation and lead to financial losses, distress, inconvenience, embarrassment, loss of information privacy, threats to personal safety, and crime.

2.4 Flexible working, where users work from home, presents additional risks to information as small computing equipment and storage devices are easily lost or stolen or connected to an insecure computer or network.

2.5 Therefore, PSCA needs to set out rules of acceptable use of all forms of electronic communication, the consequences of misuse and the measures that will be taken to monitor compliance with the policy.

3. Relevant Legislation

3.1 Both line managers and individuals have responsibilities regarding the legal use of electronic communications. There are now many laws and legal rules governing information and data security and some examples are shown below.

3.2 **Availability**: The Freedom of Information Act 2000 seeks to ensure that information is disclosed to the public unless an existing prohibition on disclosure exists by way of statute or through the use of an available exemption available through the Freedom of Information Act.

3.3 **Confidentiality**: The GDPR protects personal information from disclosure: an individual might commit a criminal offence by disclosing personal information without the authority of the organisation. Also there are duties of confidentiality under common law.

3.4 **Integrity**: The GDPR requires that personal information is adequate, relevant, is not excessive and is accurate.

4. Breaches of the Data Handling and Electronic Communications Policy

4.1 Any unusual occurrence, which might indicate the presence of a computer virus, or a clear breach of security whilst using electronic communications, must be reported immediately to ICT Support.

4.2 The user's line manager should be notified immediately if any of the rules specified in this policy are broken inadvertently, in order to avoid or mitigate disciplinary action for breaching the policy.

4.3 Actions or neglect leading to a breach of this policy by an employee could result in disciplinary action.

4.4 Breaches of this policy by a user who is not a direct employee of PSCA may result in action being taken against the user or his or her employer.

5. General Requirements for All Users

5.1 This policy applies to all users, at all times and in all locations where PSCA computer network or equipment is used, or school information is accessed.

5.2 PSCA operates within the law at all times and the following points must be observed;

- Information must not be saved on the computer network or uploaded onto the Internet in breach of copyright.
- Intellectual property rights and import / export regulations must not be breached.
- All copies of computer software used must have a current licence the purchase of which must be auditable; the source of free and evaluation software must be documented.
- Personal information must only be stored on the system if the purpose for which the data is held is covered by PSCA's notification under the General Data Protection Regulations..
- The requirements of the Freedom of Information Act 2000 must be complied with.
- Confidential and personal information must be protected appropriately at all times and particularly when it is transmitted electronically outside the school or stored on mobile computing or storage devices.
- Confidential and personal information must not be uploaded onto the Internet or any other network without suitable protection being in place.
- Confidential or personal information must not be displayed on an unattended PC screen.
- Users must not attempt to access a system for which they have not been given authority.
- Users must not deliberately access or use any form of malicious software.
- Users shall not watch live television on any device owned by PSCA without management approval (managers must ensure that a valid television licence is held or is not required).
- Hand held mobile phones or any other devices must not be used to send or receive phone calls, texts, emails or to access the Internet whilst driving.

5.3 Electronic communications must not be used in any way that might be seen as inappropriate.

5.4 Electronic communications must not be used in any way that might be seen as defamatory, libellous, insulting or offensive by others, or in any way that contravenes any other PSCA policies.

5.5 Communications must not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity.

5.6 Only conventional and authorised routes to electronic communications facilities may be used.

5.7 Users must not interfere with the configuration of operating system software, including Internet Explorer or other Internet browsers, on PCs, laptops, network devices, phones or other devices.

5.8 Users shall not attempt to bypass or subvert system security controls implemented by PSCA, including the virus scanner or by installing any other software.

5.9 Software, including screen savers, must not be downloaded or installed without approval from ICT Support.

5.10 Any macros used in office automation software such as Microsoft Office must be acquired from trusted sources e.g. written in-house. If in doubt, guidance should be sought from ICT Support.

5.11 When using PSCA owned devices, access to the Internet must be made through using software and hardware provided for that purpose by ICT Support. Any exceptions to this must be formally risk-assessed and require approval by ICT Support.

5.12 Emails must be sent via PSCA's email system. Sending to and receiving mails from other users of web based accounts is allowed for business purposes, but must be considered less secure.

6. Controlling Access to computer and telephone facilities

6.1 In order to maintain full accountability, each user shall have an individual user name and password, which shall not be shared with others. Similarly, individual email accounts shall not be shared with others.

6.2 Passwords used to access information or computing facilities must be kept **secret** and protected from disclosure whilst being typed.

6.3 Strong passwords, which are difficult to guess, must be used. A unique password must be used each time the password is changed.

6.4 Passwords must be changed regularly wherever possible and changed immediately if it is suspected that someone else may have seen or guessed it. Wherever possible a password must be changed on first use when it has been set or reset by someone else, e.g. a system administrator or ICT Support.

6.5 Only **authorised** people are allowed to access PSCA information, equipment or computer network. All PCs must be logged off or locked when unattended. Computing equipment shall be

positioned so that unauthorised people, including colleagues, are not able to view sensitive information. External visitors must be supervised appropriately at all times.

6.6 PSCA equipment must not be passed to anyone else without management approval and without PSCA's asset register being updated. All users who are about to leave PSCA employment must arrange for any mobile computing equipment and computer storage used to be returned to ICT Support before leaving.

6.7 All information shall be removed from all equipment before disposal. Only ICT Support approved methods of disposal shall be used.

7. Use of PSCA devices/services

7.1 PSCA owned devices or services must not be used for personal gain or profit.

8. General requirements

8.1 Computing hardware and software shall be purchased in negotiation with ICT Support. All hardware and software must be sourced from reputable suppliers to ensure that it cannot be used to introduce malicious code into PSCA's computers or computer network.

8.2 The physical security of all PSCA's equipment and information must be considered at all times and in all locations and adequate provision for secure storage of all equipment, including servers and network devices, must be made. Particular arrangements for physical security shall be made for premises outside school and when travelling.

8.3 Users shall seek management guidance before sensitive information and PSCA owned equipment is removed from school premises to ensure that adequate security controls are in place.

8.4 Laptops and other portable devices, and all forms of information storage must be locked away when not in use.

8.5 Mobile equipment must not be left in an unattended vehicle even when it is parked at the user's home. Particular care must be taken to protect mobile phones and small mobile storage devices.

8.6 Users shall not interfere with or change physical security measures introduced by ICT Support that protect against theft, tampering and unauthorised use of equipment. Users shall follow instructions and guidelines for their use.

8.7 Consideration must be given to the need for additional physical protection for critical information, such as storing in a fire and heat resistant safe when not in use.

8.8 ICT equipment, software or information that is lost or stolen should be notified to SLT as soon as possible.

8.9 Staff must make appropriate arrangements for their manager or other colleagues to access their information (e.g. school emails and voicemails) when they plan to be absent from work for a day or more.

9. Professional and courteous use of electronic communications

9.1 Users shall not use electronic communications in any way that could damage PSCA's reputation.

9.2 Users must not photograph or film by any means, including web cams and mobile phones, confidential information without management approval.

9.3 Users must not represent their own personal opinion as being that of PSCA.

10. Use of the Telephone

10.1 If confidential information is requested over the phone it must be disclosed only to authorised people. If asked for such information by phone, the user must check that the caller is who they say they are and that they are entitled to the information. Check any telephone or fax number given by the caller and call back with the information.

10.2 Exercise caution when talking on the phone. Confidential and personal information must be protected from eavesdropping during telephone conversations and when listening to voicemail messages or answering machines, by choosing a suitably private environment. Voicemail messages must not be listened to on a speakerphone.

10.3 The voicemail password on all PSCA voicemail accounts must be changed on first use.

10.4 Do not leave sensitive messages on voicemail or answering machines.

11. Use of the Computer Network

11.1 The computer network must be protected at all times. Any PC, laptop, telephone or other device must not be connected to the PSCA computer network without approval granted by ICT support. This will usually be given by the issuing of login credentials to the BYOD network.

11.2 Personally owned equipment and storage devices must only be connected to PSCA's BYOD network.

12. Non-PSCA or personally owned equipment/storage devices

12.1 Non-PSCA equipment connected to PSCA's BYOD network must have up to date and effective anti-virus software installed and activated.

13. Devices with wireless capability

13.1 Non-PSCA equipment shall only be connected to PSCA's BYOD network.

14. Anti-Virus and security patches

14.1 All PCs, laptops and other devices must have up-to-date virus checking software where applicable. Users must ensure that **all** updates to virus checking software are applied as soon as possible.

14.2 PSCA laptops and other mobile devices must be made available to ICT Support for Operating System updates and anti-virus updates when requested.

15. Use of E-mail

15.1 Users shall use best endeavours to ensure that the intended recipients of email messages are correctly identified so that sensitive information is not accidentally released to unauthorised users.

15.2 E-mail headers or message contents must not be changed when forwarding emails so as to misrepresent the views of others**; be aware that others may change emails written by you or forwarded to you**. Copies of important emails sent must be kept.

15.3 Emails must not be automatically forwarded to an email address outside of the school without protection from interception, e.g. by use of encryption.

15.4 Passwords must not be included in the text of an e-mail that refers to an attachment, which is password protected because it contains confidential or personal information. Password protecting attachment offers only very limited protection and alternative means of protection, such as encryption, must be used to protect information which is sensitive or confidential.

15.5 All external email and attachments, incoming and outgoing, must be scanned for malicious content.

15.6 Whilst every effort is made to block emails containing undesirable material, it is possible that some will still get through and all email users must accept that this may be the case.

15.7 Users must not create or forward an email chain letter or chain text message.

15.8 "Phishing" emails requesting personal information such as credit card details, user names and passwords, or containing links to Internet sites where such information is requested, must always be ignored and deleted.

15.9 Extreme care must be taken in opening attachments of external emails if they are not expected and are not from a known and reliable source. ICT Support can provide advice if it there is concern that an email or attachment might contain a virus or other malicious code.

15.10 Emails warning of viruses and other malicious code must be forwarded immediately to the ICT support. Do not follow instructions in such mails unless they are issued by ICT support, because they might be a hoax.

16. Use of Internet

16.1 Information on the Internet must be treated with caution due to the unregulated nature of public networks.

16.2 Use of online chat rooms, Instant Messaging, online computer games and gambling online is forbidden.

16.3 Text or images, which contain anything that may bring PSCA into disrepute, must not be loaded on to the Internet.

16.4 Illegal or inappropriate Internet sites must not be accessed and will be blocked wherever possible.

16.5 ICT Support should be contacted when access to blocked Internet sites is essential for business reasons.

16.6 Care must be taken when opening or downloading files from the Internet if they are not from a known and reliable source.

16.7 All internet activity logged to a user name will be deemed to have been performed by them.

17. Flexible Working

17.1 Users should use extreme caution when accessing any Personal Data but especially any data that falls within Special Categories of Data, or is of a sensitive or confidential nature, whilst in places accessible to unauthorised users, e.g. whilst travelling by public transport.

17.2 Use of removable media devices increases significantly the risk of malicious software being introduced and of information being inappropriately disclosed, accordingly suitably secure online storage media (e.g. Google Drive, Office 365/OneDrive, Apple iCloud, DropBox, etc.) will be used wherever possible.

17.3 All PSCA and non-PSCA computing devices, which are used for the processing of PSCA Personal Data must be password or PIN protected and this must be enabled on all mobile devices.

17.5 All users must be advised how to create strong passwords.

17.6 Users should notify ICT Support at the earliest possible opportunity if they experience an operational problem with PSCA owned mobile computing facilities or equipment and arrange for affected equipment to be inspected by ICT Support if required.

18. Encryption Policy

18.1 Encryption is a means of scrambling information so that only authorised people with the correct key can read it. This encryption policy applies to all types of mobile devices which contain computer readable information storage.

18.2 This policy includes devices with computer-like functionality, which can manipulate information, and also to storage only devices. These include, but are not restricted to;

- Laptops
- Tablet PCs
- Mobile & "smart" phones
- Digital camera
- MP3 and MP4 players
- USB memory sticks
- Tapes, CDs and DVDs
- External hard disks.

18.3 Wherever technically feasible, encryption software shall be installed on **all** new mobile devices. ICT Support will decide if encryption software is technically feasible. Where encryption software is not technically feasible, an individual information risk assessment must be completed to determine if it is acceptable to store the information unencrypted.

18.4 All information held on existing mobile devices shall be assessed for its need for confidentiality. With the proviso regarding technical feasibility detailed above, encryption of information on mobile devices and storage is mandatory in the following situations:

- The information held is defined as "**personal**" or "special category data" under the GDPR.
- The information held is **commercially sensitive.**
- Where any of the information held might be **prejudicial** to PSCA's reputation were it to be inadvertently disclosed.
- The device or storage contains emails. This is because emails often contain information classified as "**personal**" or "special category data" under the GDPR and the user has no control over the content of emails sent to him or her.

18.5 ICT Support shall evaluate and provide standard encryption products for each type of mobile device and each level of security required. All encryption products used must be approved by ICT Support.

18.6 Where information is of a particularly sensitive nature, a more robust encryption product shall be considered - this is one that has been independently and formally evaluated against government defined security criteria.

18.7 Under normal circumstances all confidential, sensitive and personal information should be stored on network servers, however in exceptional circumstances if such information is kept on desktops, an exception to policy would be required by completing a risk assessment and ensuring the PC has full disk encryption.

18.8 PSCA retains the right to decrypt and examine all encrypted information on PSCA devices.

19. Reporting Security Incidents and Software Malfunctions

19.1 An event that causes loss or damage to PSCA information, or an action that is in breach of any PSCA PSCA security policy, including this policy, should be reported immediately to ICT Support and SLT..

19.2 Users shall immediately notify their line managers and ICT Support of any suspected or actual security incidents, weaknesses or software malfunctions, i.e. any event that causes, or could cause, loss or damage to PSCA information, or an action that is in breach of any PSCA security policy, including this policy.

19.3 Evidence associated with a security incident must not be tampered with or deleted until authorised by the user's line manager or ICT Support. Under no circumstances should an attempt be made to replicate or simulate any suspected security threat or weakness, as the attempt could be deemed as misuse of the computer system.

19.4 Users must not attempt to correct a software malfunction by for example, removing the suspected software or by changing any software settings within or outside the software package. The user must immediately seek advice from the ICT Support. Any portable media such as diskettes or CDs used on the affected computer must not be used on any other computer to ensure the software malfunction is not inadvertently spread to other computers or the computer network.

19.5 Suspected malicious software must be reported immediately to ICT Support by telephone (not email), and work ceased on the PC or other device.

20. Personal Use of the Internet

20.1 Users are trusted to use the Internet responsibly recognising that school business is a priority and that the network must be protected from unreasonable and excessive personal use. Managers are responsible for ensuring that all users understand that this is a condition of allowing personal use.

20.2 If personal use of the Internet causes problems with business access, personal use might be withdrawn. All conditions of use in this policy must be complied with during personal use and some of the key ones are repeated here for emphasis.

20.3 PSCA provides ICT facilities for school business. Personal use of the Internet is allowed in **non-work time** where there is no effect on the performance, effectiveness or timekeeping of the individual in performing their duties and no impact on others' business use of the Internet.

20.4 ICT Support provides support for business use and it must **not** be contacted for queries concerning personal use of the Internet.

20.5 The Internet must not be used in any way that might be seen as defamatory, libellous, insulting or offensive by others, or in any way that contravenes any PSCA policies. Communications must not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity.

20.6 PSCA accepts no responsibility or liability whatsoever for problems of any kind caused to or by users arising from personal use, for example (but not limited to) when buying goods online, including identity theft and compromise of credit card numbers.

20.7 All users are responsible for reducing the risk of downloading malicious code, such as viruses and spyware (code that is secretly installed and can be used to steal bank or credit card details). To do this all users must check that the anti-virus software on their PC is kept up to date either automatically for desktop PCs or on laptops by requesting an update when connected to the network. Whilst the anti-virus software should be updated automatically on desktop PCs, now it is important that this is checked regularly.

20.8 Some web sites are more likely to contain malicious code than others. It is very difficult to provide specific guidance on this but large reputable companies and organisations make every effort to protect their web sites from malicious code. Users are expected to use their common sense to keep the risk of malicious code to a minimum. If a PC malfunctions in any way, this must be reported to the ICT Support immediately because it might be an indication of infection by malicious code.

20.9 Personal information, bank details, usernames and passwords must **not** be included in an automated log on routine, e.g. where there is a check box to "remember password?" this must **not** be checked. If this were done, another user on the same PC might be able to gain access to personal banking or other accounts.

20.10 The downloading of video, music or online games for personal use is not allowed. Non-work related data must not be stored on the network servers without management permission and anything downloaded must be legal. Large volumes of information for personal use must not be downloaded from the Internet as it might impact on Internet performance for business use.

20.11 Inappropriate Internet sites will be blocked wherever possible.

20.12 The Internet must not be used for personal gain or profit.

20.13 Privacy of any communications cannot be guaranteed. All monitoring will be fair and proportionate to the risks of harm to PSCA's reputation and the information stored on the system, and undertaken so as to intrude on users' privacy only as much as is necessary.

20.14 Users are reminded that actions or neglect leading to a breach of this policy by an employee could result in disciplinary action; this could include dismissal without notice even for a first offence if sufficiently serious. Breaches of this policy by a user who is not a direct employee of PSCA may result in action being taken against the user or his or her employer.

21. CCTV

21.1 PSCA uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for students, staff and visitors, and to prevent the loss or damage to school property.

21.2 The system comprises a number of fixed and dome cameras without sound recording capability.

21.3 The CCTV system is owned and operated by PSCA, the deployment of which is determined by PSCA's leadership team.

21.4 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the school community.

21.5 PSCA's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998.

21.6 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the school data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

21.7 CCTV warning signs will be clearly and prominently placed at all external entrances to PSCA including school gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV. In areas where CCTV is used, PSCA will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

21.8 Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated. PSCA will ensure that the location of equipment is carefully considered to ensure that images captured comply with the data protection laws..

21.9 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

21.10 PSCA may in exceptional circumstances set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;

ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances authorisation must be obtained from a member of the senior leadership team. Covert monitoring must cease following completion of an investigation. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles.

21.11 Individuals have the right to request access to CCTV footage relating to themselves under the GDPR. All requests should be made in writing to the Data Protection Officer (dpo@schoolofcreativearts.co.uk). Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location. PSCA will respond to requests without delay and at the latest within one month of receipt. PSCA will be able to extend the period of compliance by a further two months where requests are complex or numerous. Individuals will be informed if and why a extension is necessary. There will be no charge for any requests for access unless a request is manifestly unfounded or excessive, particularly if it is repetitive. The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

21.12 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and PSCA's service providers where these would reasonably need access to the data (e.g. investigators). Requests should be made in writing to the Data Protection Officer

22. Monitoring of this Policy

Monitoring of this policy will be;

22.1 To ensure that this policy is adhered to and to detect and investigate unauthorised use of electronic communications.

22.2 To maintain the effectiveness, integrity and security of the network.

22.3 To ensure that the law is not being contravened.

22.4 To protect the integrity and reputation of PSCA and the services it provides.

22.5 All monitoring will be fair and proportionate to the risks of harm to PSCA's reputation and the information stored on the system.

22.6 Undertaken so as to intrude on users' privacy only as much as is necessary.

22.7 Carried out similarly regardless of whether the user is office based or working remotely.

22.8 Carried out subject to the requirements of legislation. Access to any records of usage will be stringently controlled.

23. Suspected misuse of the PSCA's equipment, network and/or breaching this policy

23.1 Where PSCA has received a complaint or reasonably suspects that a user is misusing the PSCAs equipment, network and/or is in breach of this policy, then any relevant device may be examined by appropriate management and/or ICT Support and may be surrendered for this purpose upon request.

23.2 All PSCA hardware and software remains PSCA's property at all times and must be made available for inspection immediately upon request.

24. Monitoring and Review

24.1 PSCA will review this policy at least annually and more often when legislation and guidance changes. The Governing Body will determine how often the policy will be re-issued or amended.

24.2 Its implementation and effectiveness will be monitored by the DPO and the Digital Team.

24.3 The policy will be promoted and implemented throughout PSCA.