Enhancing Lives,
Connecting Communities

Information Security Policy

1 Introduction

1.1

Scope

This document sets out PKAVS' Information Security Policy, and the responsibilities of everyone using PKAVS' systems and IT. Information security is of great importance to the PKAVS, allowing it to protect service users, employees, and volunteers, ensure compliance with legislation, and demonstrate that PKAVS understands and applies proportionate guidance and process to recording, storing, processing, exchanging, and deleting information. Should this not be achieved PKAVS can risk, at worst, the safety of individuals, loss of financial information, breach of commercial confidentiality, loss of public confidence, and subsequent financial penalties from the Information Commissioner's Office.

1.2

Definition

In this policy, *'information security'* is defined as *Preserving the availability, confidentiality, and integrity of the physical assets and information assets of PKAVS.*

Preserving

This means employees, volunteers, third parties, and any external parties have to preserve information security, to report security breaches, and to act in accordance with the requirements of the Information Security Policy. All employees and volunteers will receive information security awareness information and more specialised employees will receive appropriately specialised information security training.

the availability,

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and PKAVS must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, and information. There must be appropriate Business Continuity Plans.

confidentiality

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to PKAVS information and its systems (including its network(s), website(s), storage systems, and third party IT applications).

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate data backup plans and security incident reporting. PKAVS must comply with all relevant data-related legislation, namely the UK Data Protection Act 2018; GDPR; The Computer Misuse Act 1990; Copyright, Designs, and Patent Act 1988; Privacy and Electronic Communications Regulations; and any other relevant regulatory frameworks.

of the physical assets

The physical assets of PKAVS including, but not limited to, computer hardware, data cabling, telephone systems, filing systems, and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), PCs, laptops, mobile phones and mobile devices, as well as on USB sticks, flash storage, and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

of PKAVS.

A **Security Breach** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality, or integrity of the physical or electronic information assets of PKAVS.

2 Policy Statement

2.1

It is the policy of PKAVS to ensure that all information systems operated by the organisation are secure. It is also the aim of PKAVS that all staff must be fully aware of the need to maintain secure systems and fully understand their responsibilities as outlined in this document.

All staff and volunteers are responsible for ensuring that they understand and abide by this policy. Failure to do so will be viewed as a serious matter and may result in disciplinary action in line with PKAVS' Code of Conduct Policy.

It is the policy of PKAVS to ensure:

- Information is protected against unauthorised access.
- Confidentiality of information is maintained.
- Information is not disclosed to unauthorised persons through deliberate or negligent action.
- The integrity of information is maintained by protection from unauthorised modification.
- Information is available to authorised users when needed.

- Regulatory and legislative requirements are met.

- Contingency plans are produced and tested as far as is practicable to ensure business continuity is maintained.

- Information Security materials are provided for all staff.

- All breaches of information security and suspected weaknesses are reported, investigated, and appropriate action taken.

- Sharing of information with other organisations/agencies is permitted providing it is done within the remit of a formally agreed information sharing procedure.

- That there is a fair and consistent approach to the enforcement of standards of conduct expected from employees when using social media sites.

3 REQUIREMENTS

For the avoidance of doubt, the Information Security Policy requires that;

- Individuals must ensure that, as far as is possible, no unauthorised person has access to any data held by PKAVS.
- Individuals must ensure that physical security measures are properly used.
- Individuals must not deliberately or negligently corrupt, damage or destroy data, software or hardware belonging to PKAVS. This includes the proliferation of viruses or other similar computer programmes.
- Individuals will be given access passwords to certain computer systems. These must not be disclosed to other members of staff or volunteers. They should not be written down and they should be changed regularly.
- Individuals must not load or download software packages onto PKAVS' PCs (without IT Administrator approval) and under no circumstances should games software be loaded on PKAVS' PCs/devices (unless appropriate for service delivery objectives).
- Any staff found to be storing large numbers of non-work related files, especially large files such as photographs or videos, may be asked to remove them and, if they continue to breach the requirement, may be the subject of disciplinary action.
- Any files received on any media, brought or sent into PKAVS, or files received by electronic mail must be virus checked before being loaded onto a PKAVS' PC/device.
- All employees and volunteers must read, understand, and sign to acknowledge that they have read and accepted this Policy and the specific requirements of it, which are as follows.

3.1

Network Security

- Only PKAVS owned Laptops and PC's are allowed to be connected to PKAVS corporate network.
- If remote access is required specific permission must be sought from the employee/volunteers' line manager and requested from PKAVS' Privacy Officer or PKAVS Business Support Function.

3.2

Physical Security

- Access to data held on PKAVS' information systems is minimised by restricting physical access to the PKAVS' offices.
- Where information is kept in PKAVS' offices, access to buildings is restricted by ensuring that doors are locked when not in use, closed properly, and that entry codes are kept secure and changed regularly.
- Doors and windows must be secured overnight and at all times when the office is left unattended.
- Visitors to PKAVS' buildings must be accompanied at all times and signed in and out of the premises on arrival and departure.

3.3

Computer Security

3.3.1

Data Storage

- All staff must abide by PKAVS' GDPR Policy and the Computer Misuse Act.
- Storage of data on PC or Laptop's C: drive (local drive) is discouraged and all users are requested not to store files on this drive as in the event of failure, all data stored on the drive would be lost.
- All information related to PKAVS' business is to be stored on the personal network drive (the U:\ drive) or on PKAVS' shared drives. This is a secure storage area which is regularly backed up and is therefore resilient to failure.
- The following types of file can only be stored if they relate to explicit business needs.

  File Type Description:

  .AVI Movie Files; .MPG Movie Files; .MPEG Movie Files; .MP3 Sound Files; .MP4 Sound Files; .M4A ITunes Files

  .MOV Movie Files; .EXE Executable files

3.3.2

File Storage and Naming Conventions

- All documents and files should be given clear and descriptive titles that will help others to understand what is contained within them.
- Information which is no longer required should be promptly disposed of by deletion or destruction. Unless an audit record of versions is explicitly required, previous versions of documents should be destroyed when the new version is created.

3.3.3

Screen Locking

- Computers must not be left unattended with the screen unlocked when logged in to PKAVS' network.
- Whenever staff/volunteers move away from a workstation they must ensure that they have logged off or locked the PC/laptop.
- When leaving a place of work staff must ensure they have logged off and have closed down the PC/laptop correctly.

3.3.4

Memory Sticks and removable media

- Only PKAVS supplied encrypted memory sticks are to be used. These will be supplied centrally and a record of distribution held.
- Sensitive data or personal information must not be transferred to a home PCs/laptops.
- No member of staff or volunteer should install unauthorised software on PCs/laptops.

3.3.5

Passwords

- Passwords given to you are for your use only.
- Passwords should not be written down or given to others to use under any circumstances.
- Passwords must be a minimum of 7 case sensitive characters and should be a combination of upper/lower/numeric/special characters. Ideally Passwords should also contain random characters such as #@?!$& etc. Passwords must include at least three different character types.
- Password should be significantly different from personal passwords.
- Passwords must be changed every 90 days as a minimum.

3.3.6

Viruses

- All files received on remote media from outside PKAVS or received via electronic mail must be checked for viruses before being used on PKAVS' equipment. You must not intentionally introduce/send or download files or attachments which contain viruses, or which are meant to compromise the PKAVS' systems.
- If a virus is suspected, PKAVS Business Support Function must be informed immediately. The workstation should not be used until given permission from the IT Administrator and a sign stating this should be placed on the workstation to warn other users. Any storage devices that have been used on the suspected infected workstation should be gathered together and not used.

3.3.7

Printing

- Staff must ensure adequate care is taken when printing information. If there is a printer fault when printing material containing sensitive or personal information contact PKAVS Business Support Function who will ensure that any unprinted files are deleted from the print queue.

- Sensitive printed materials must be removed from the printer tray immediately; if a large volume of sensitive material is printed the employee/volunteer should monitor printing at the printer itself.

3.3.8

Scanning

- Staff must ensure adequate care is taken when scanning documents and using PKAVS' scanning solution, checking the destination location or email address.

3.4

Clear Desk

- All manual files and paper records must be locked away before leaving the office. Where this is not possible or where offices employ "open" shelving for the storage of files and documents, offices must be locked when left unattended.
- All sensitive and personal information must be held securely in locked containers, lockers, drawers, and filing cabinets to prevent unauthorised access.
- All sensitive and personal waste must be disposed of securely. Waste shall be shredded or placed in the appropriate confidential containers for secure disposal.

3.5

Mobile Workers and Home Workers

3.5.1

Laptops

- Care must be taken to avoid being overlooked whilst using PKAVS' equipment in any public area
- Laptops must be kept in a secure location when not in use.
- Laptops must not be left unattended during the normal working day unless it is on PKAVS' premises where there is good physical security.
- When using portable equipment on the move, or outside of office hours, reasonable care should be taken to secure it.

3.5.2

Manual Files

- Manual files processed outside of PKAVS' property must be kept with the individual completing this work.
- When left unattended, manual files must be in a locked container and out of view.
- Computer equipment or manual files that are travelling with an employee must be locked in the boot of the car or kept with the individual at all times when travelling by public transport.
- Computer equipment or manual files must not be left unattended on a train or bus, or left in a vehicle overnight.

3.5.3

Mobile Telephones and Mobile Devices

- Staff and volunteers issued with mobile phones, tablets, or other personal digital equipment are responsible for safekeeping and security.
- Security lock and pin protection must be used where available to protect the device and any stored data.
- PKAVS-issued mobile devices are provided for work-related purposes only.

3.5.4 Lost or Stolen Mobile Devices

- If a mobile device is lost or stolen, staff and volunteers must;

1) Contact the Finance Office immediately to report the loss and ask for the mobile device to be suspended so that it can no longer be used.

2) Notify the local Police Station of the loss if a theft has occurred.

3) Refer to PKAVS Data Breach Procedure immediately if there is any possibility personal information is compromised.

- If a laptop or tables is lost or stolen, staff and volunteers must;

1) Contact their Line Manager immediately to report the loss.

2) Notify the local Police Station if a theft has occurred.

3) Refer to PKAVS Data Breach Procedure immediately if there is any possibility personal information is compromised.

3.5.5

Leaving PKAVS or Moving Into another Role

- Staff who are issued with laptops, mobile devices, or storage devices must ensure their safe return on termination of employment or acceptance of a different post within PKAVS which does not require the use of those devices.

3.6

Use of the Internet

3.6.1

Downloading of Information Resources

- Individuals must not download non-work related information from the Internet during working hours. To reduce the likelihood of a virus infection, individuals must take care to ensure that the files are from a trustworthy source.
- During designated break periods staff/volunteers limited personal use of the internet is permitted. All internet use is monitored and accessing pornographic or other unsuitable material is strictly prohibited (unless it is deemed part of your role) and would be considered a serious disciplinary matter which may result in dismissal. If you have any doubt, please speak with your line manager.

- Software must not be downloaded and/or installed onto PKAVS' IT equipment unless it has been approved by the IT Administrator and can be validated that it is licensed for current use.
- Staff/volunteers are reminded that copyright laws apply to the Internet and care must be taken should there be a need to re-use any information (including images) in any PKAVS' work.

3.6.2 Uploading Data / Information to the Internet

- Any staff/volunteers who are responsible for uploading data/information to the internet (including websites, social media, etc.) must be sure that the information being uploaded is suitable to upload. PKAVS' Social Media Policy guides the use of social media within PKAVS for work and personal purposes.

3.6.3

Internet Filtering and Blocking

- Users should not attempt to by-pass the PKAVS internet filtering software.
- Staff who encounter a commonly used business site which is blocked and have genuine business reasons for accessing that site frequently may contact PKAVS Business Support Function and request the site is on an approved list of websites.

3.7

E-mail Use

This section sets out the expectations for all PKAVS staff/volunteers who are provided with access to Outlook/Office 365. Outlook/Office 365 is provided as a business tool and should not be used for non-work related matters.

3.7.1

Sending email

- Email should only be used for business purposes.
- A corporate disclaimer is applied to all outgoing messages.
- All e-mails must have the subject line completed and should be checked for accuracy of spelling, punctuation, and grammar. Bold text should only be used sparingly, and for emphasis, and underlining should only be used for links. The use of upper case text should be avoided as this may be interpreted by recipients as shouting.
- To avoid information overload, individuals should consider carefully who needs to be included in any e-mail and whether face-to-face or telephone contact could be an alternative method.
- Staff/volunteers should only "reply-to-all" if appropriate and consider when it might be more useful to respond only to the original sender or a select number of recipients.
- When sending sensitive e-mail, individuals should be mindful of any permissions that recipients may have set up, such as re-distribution or message forwarding.
- Individuals must not alter the text of any received messages, including when forwarding them to others. Similarly, individuals should not assume that a forwarded message matches what was originally authored.
- Individuals must not use other peoples' e-mail accounts nor attempt to impersonate someone else or appear anonymous when sending an e-mail.
- All emails should be finished with an email signature that includes your name, title, hub/service, contact details, PKAVS' logo, and PKAVS' charity/company statement.
- User should be aware that email communication may be recorded

3.7.2

Agreements by email

- Individuals must take care not to enter into any agreements via e-mail that could constitute a contract, and if in doubt must seek the advice of PKAVS' HR Function, Finance Department, or Chief Executive.

3.7.3

Mailbox size and housekeeping

Each mailbox will have a designated owner who will be responsible for housekeeping (archiving or deletion) all types of items. Once the mailbox limit is reached, users of that mailbox will not be able to send or receive any further mail and therefore housekeeping must be planned well in advance of reaching the space limit.

3.7.4

Distribution lists

- Mail distribution lists are provided to enable business communications to be made to groups of individuals. Lists should only be used for related business purposes, and any queries related to their use or composition should be discussed with senior managers.

3.7.5

Mailbox management

- Staff/volunteers are expected to treat their mailbox like an electronic in-tray, ensuring that it is regularly checked and that messages requiring further action are dealt with promptly – including sending holding responses where appropriate.
- Individuals should only archive and retain messages that need to be kept and these should be selected in line with business needs and any PKAVS' retention schedules. All other e-mail that does not constitute a necessary record of business should be deleted once it is no longer required.
- When an email is received with an attachment which needs to be retained, individuals should save the attachment to the network drive, and not leave the attachment within the email.

3.7.6

Misuse of email

- Individuals must not send or forward any abusive, threatening, defamatory, or obscene messages. Likewise, individuals should avoid sending messages in the heat of the moment, taking time to reflect on drafts, and how they may be interpreted before sending them.
- Staff/volunteers must take care with any suspected malicious or nuisance e-mails received (e.g. chain email, hoax, and spam e-mails) and delete them. If any suspicious e-mails are received they should be reported to PKAVS Business Support Function.
- Individuals must never open attachments to an e-mail of unknown origin as they may contain viruses and other malware.

3.7.7

Mail and absence

- An "Out-of-office" notice must be used whenever an individual is away on annual leave or for an ongoing period of time, and messages should clearly indicate a date of return and contact details for those who can deal with issues whilst the individual is away.

Document Control

PKAVS’ Privacy Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.

A current version of this document is available to all members of staff on the corporate network or on request.

This procedure was approved by the Chief Executive Officer on 22/05/18 and is issued on a version controlled basis under his/her signature.

Signature: Paul Date: 22/05/18

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	PKAVS CEO	22/05/18
2	Small Updates	PKAVS Privacy Officer	31/01/20