Information Security Policy

This document refers to JPN Training terms and conditions in regard to the organisation's information security policy.

Company Name:	JPN Training
Approver (Date):	Julia Palmer-Ndu – 28/07/2026
Review due date:	July 2027
Current Version:	1.0
Update history:	28/07/2026 Document Creation
Document Type	Internal Employees
Classification	Internal Use Only

1. Access Control

1.1
Staff, Members and contractors should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

1.2

Formal procedures will be used to control access to systems. An authorised manager must raise an IT Service Request on Sinbad for each application for access. Access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Managers must ensure they advise IT of any changes requiring such modification/removal.

1.3

Staff, Members and contractors must comply with JPN Training Service's IT Policy in relation to passwords.

1.4

Line managers must ensure that passwords to local systems are removed or changed to deny access. This would apply where, for example, the system is externally hosted and not under the remit of IT.

1.5

Where appropriate, staff working out notice are assigned to non-sensitive tasks or are appropriately monitored.

1.6

Particular attention should be paid to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals & documents.

1.7

Once an employee has left, it can be impossible to enforce security disciplines, even through legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

1.8

System administrators will delete or disable all identification codes and passwords relating to members of staff who leave the employment of JPN Training on their last working day. The employee's manager should ensure that all PC files of continuing interest to the business of JPN Training are transferred to another user before the member of staff leaves.

1.9

Managers must ensure that staff leaving JPN Training employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to JPN Training information and equipment.

1.10

All visitors should have official identification issued by JPN Training il. If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

1.11

There is a requirement for system administrators to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. IT Services will advise on the most suitable control.

1.12

Physical security to all office areas is provided through the access control system. Staff should challenge strangers in the office areas without an ID badge. Never let someone you don't know or recognise to tailgate you through security doors.

2. Security of Equipment

2.1

Portable computers must have appropriate access protection, for example passwords and encryption and must not be left unattended in public places.

2.2

Computer equipment is vulnerable to theft, loss, or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.

2.3

Due to the high incidence of car thefts laptops or other portable equipment must never be left unattended in cars or taken into vulnerable areas.

2.4

Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off JPN Training property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

2.5

Staff working from home must ensure appropriate security is in place to protect JPN Training equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring JPN Training equipment and information is kept out of sight.

2.6

JPN Training issued equipment must not be used by non-staff personnel.

2.7

All of the policy statements regarding the use of software apply equally to users of portable equipment belonging to the JPN Training.

2.8

Users of this equipment must pay particular attention to the protection of personal data and commercially sensitive data. The use of a password to start work with the computer when it is switched on, known as a 'power on' password, is mandatory and all sensitive files must be password protected if encrypting the data is not technically possible. The new user will refer to the instruction book to learn how to apply these passwords or may make arrangements for basic training in the use of a portable computer.

2.9

Users of portable equipment away from JPN Training premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged and take appropriate precautions to minimise risk of theft or damage.

2.10

Staff and Members who use portable computers belonging to JPN Training must use them solely for business purposes otherwise there may be a personal tax/National Insurance liability.

3. Payment Card Industry (PCI) Compliance

3.1 DSS Compliance

JPN Training is currently PCI DSS compliant; the Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store or transmit credit or debit card information maintain a secure environment.

3.2 Failure to Comply

Failure to comply with these standards could lead to fines or even the removal of the JPN Training ability to accept card payments.

3.3 Cash Receipts

Those users who have access to any part of the JPN Training Cash Receipting systems whereby they are taking payments either in person or over the phone should only enter Card numbers into the relevant Capita payment screens and under no circumstances should Card Holder data such as Card Numbers be written down or copied by anybody as this would breach our PCI compliance.

4. Security and Storage of Information

4.1

All information, whether electronic or manual, must be stored in a secure manner, appropriate to its sensitivity. It is for each service area to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:

- Paper files stored in lockable cupboards or drawers
- Laptops stored in lockable cupboards or drawers
- Electronic files password protected or encrypted
- Restricted access to IT systems
- Computer screens to be 'locked' whenever staff leave their desk
- Removable media to be kept in lockable cupboards or drawers and information deleted when no longer required
- Paper files removed from the office (for site visits or when working from home) to be kept secure at all times and not left in plain sight in unattended vehicles or premises
- Laptops must never be left in unattended vehicles
- It is advisable that paper files containing personal or sensitive data are kept separate from laptops, particularly when working from home
- At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive. Access to this type of information must always be through JPN Training' network.
- To preserve the integrity of data, frequent transfers must be maintained between portable units and the main JPN Training computer system.
- Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information.

5. Clear Desk Policy

5.1

Employees are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers and cupboards as appropriate.

5.2

Although security measures are in place to ensure only authorised access to

office areas, employees should ensure that documents, particularly of a confidential nature are not left lying around.

5.3

Employees must ensure that documents are carefully stored. When properly implemented, this clear desk policy also improves efficiency as documents can be retrieved more easily.

6. Posting or Emailing Information

6.1

If information is particularly sensitive or confidential the most secure method of transmission must be selected. The following procedures should be adopted as appropriate, depending on the sensitivity of the information.

6.2

Please consider the risk of harm or distress that could be caused to the customer if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

6.3

It is important that only the minimum amount of personal or sensitive information is sent, by whichever method is chosen.

6.4 Email Correspondence

Sending information by email:

- Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes.
- If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list. Both of these options can be found in Outlook under 'file', 'options' and 'mail'.
- Take care when replying 'to all' – do you know who all recipients are and do they all need to receive the information you are sending.

- If emailing sensitive information, password protect any attachments. Use a different method to communicate the password eg telephone call, messenger or text.
- Consider the use of secure email where this is available, or use drop off and encrypt the document.
- Person identifiable data files must not be sent via email to a user's personal mailbox. Staff working from home should only access information via the JPN Training' network.

6.5 Sending by Post

Sending information by post should be carried out as follows:

- Check that the address is correct
- Ensure only the relevant information is in the envelope and that someone else's letter hasn't been included in error
- If the information is particularly sensitive or confidential, discuss the most secure method of delivery with the Post room, this could be by Special Delivery or even courier.

6.6 Printing and Photocopying

Printing and Photocopying protocols:

- All printing must be via the MFP printers
- Consideration must be given to using the Print Room for large print runs, especially where personal information is concerned.
- When printing or photocopying multiple documents, ensure you separate them when you return to your desk.
- If the copier jams please remove all documents – if the copier remains jammed report it but leave your contact details on the copier so that once it has been fixed any remaining copying can be returned to you. If possible, cancel your print run.
- Make sure your entire document has copied or printed – check that the copier has not run out of paper. This is particularly important when copying or printing large documents. Please bear in mind the printer will sometimes pause in the middle of a large print run
- Do not leave the printer unattended when you're using it – someone else may come along and pick up your printing by mistake.
-

7. Redacting

7.1

If it is necessary to redact information, either before sending it out or posting it onto the website, ensure a suitable and permanent redaction method is used
13.2 The use of black marker pen is not a suitable method of redaction
13.3 It is not advisable to change the colour of text (e.g. white text on a white background) or use text boxes to cover text as these can be removed from electronic documents. However, if this is the only option, once redacted the document should be printed and then scanned as a PDF before being sent.

8. Sharing and Disclosing Information

8.1

When disclosing personal or sensitive information to customers, particularly over the phone or in person, ensure you verify their identity. Service areas dealing with customers on a daily basis should have suitable security questions which must always be used. If in doubt ask for suitable ID or offer to post the information (to the contact details you have on file).

8.2

If a request for disclosure of information is received from a third party, you must:

- Obtain written consent from the customer that they are acting on their behalf Verify their identity, particularly if they request information via the telephone or in person. It is preferable to telephone the person back, using a recognised telephone number for their organisation (for example 101 for the Police). Do not take their mobile number and use that.

8.3

In all circumstances, you must ensure you are legally able to share the information being requested and only share the minimum amount of information necessary.

9. Retention and Disposal of Information

9.1

Information must only be retained for as long as it is needed for business purposes, or in accordance with any statutory retention period.

9.2

Staff should refer to the JPN Training Data Protection Compliance Policy and WEEE Compliance Policy for further information. The Schedule sets out the type of information held in service areas, together with statutory or agreed retention periods. Please contact the Managing Director or Administrator for further advice on retention.

9.3

When disposing of information please ensure the most appropriate method is used. Paper files containing personal or sensitive information must be disposed of in the confidential waste bins. Electronic information must be permanently destroyed.

9.4

When purchasing new computer systems or software, please consider requirements for the retention and disposal of information and ensure these are included at the scoping stage.

9.5

All information destroyed in accordance with the WEEE Compliance Policy must be logged on the Disposal Log.

10. Vacating Premises of Disposing of Equipment

10.1

It is important that a process is in place to ensure all JPN Training information is removed from premises should they be vacated and from equipment before it is disposed of. Equipment includes cupboards and filing cabinets as well as computers or other electronic devices.

10.2

The disposal of computer or other electronic devices is referenced in Section 25 of this policy and all electronic equipment must be returned to IT to be properly disposed of in accordance with JPN Training WEEE Compliance Policy.

10.3

If JPN Training vacates any of its premises, the manager of the service area occupying the premises must undertake appropriate checks of all areas, including locked rooms, basements and other storage areas, to ensure all JPN Training information is removed. Such checks should be documented, dated and signed.

10.4

If information is bagged for disposal (whether confidential or not), this must be removed before the building is vacated.

10.5

Cupboards and filing cabinets must be checked before their disposal to ensure they contain no documents or papers. If a cupboard or cabinet is locked and no key is available, Campus should be asked to open it in order that it can be checked.

11. Cloud Storage Solutions

11.1

The use of cloud storage solutions (Google Drive, Onedrive Personal, iCloud etc.) for the transfer of JPN Training information is expressly forbidden. The IT service can provide you with access to its secure Onedrive for Business for the sharing of files.

12. Systems Development

12.1

All system developments must comply with the JPN Training IT Protocols and Policies. All system developments must include security issues in their consideration of new developments, seeking guidance from the IT Administrator and Internal Audit, where appropriate.

12.2

Privacy Impact Assessments (PIAs) should be carried out prior to the purchase of any new system which will be used for storing and accessing personal information.

13. Network Security

13.1

JPN Training will engage a third-party specialist to routinely review network security.

14. Risks from Viruses

14.1

Viruses (including malware and zero-day threats) are one of the greatest threats to the JPN Training' computer systems. PC viruses become easier to avoid with staff and members aware of the risks with unlicensed software or bringing data/software from outside JPN Training. Anti-virus measures reduce the risks of damage to the network.

14.2

IT Services centrally maintain and update the currency of the virus definition files on servers, but users are responsible for checking that virus updates are automatically occurring on all desktop machines. Advice and support is available from IT Services if any remedial action is necessary. Any suspected virus attacks must be reported using the organisations Breach Management Protocol alongside being logged in the Breach Log.