IT Policy

Policy Statement

Heydays Care and Support Services regards the integrity of its computer system as central to the success of the organisation. Its policy is to take any measures it considers necessary to ensure that all aspects of the system are fully protected. This policy aims to comply with the requirements of both the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

Procedure

- Overall computer security is the responsibility of the HR officer reporting to the managing director. Line managers are responsible for security within their own departments.
- Job applicants will be questioned on their computer experience. The implications of their software knowledge will be discussed with the HR officer before a job offer is made. All references will be checked.
- On induction employees will be given copies of the computer security policy and will receive written instructions on security procedures and Heydays Care and Support Services responsibilities under the DPA and the GDPR.
- Managers are responsible for ensuring that all such workers receive the information referred to in point 3.
- Computer training at every level will emphasise the importance of security. Staff will receive a detailed statement on the implications of the DPA, the GDPR and the Computer Misuse Act 1990.
- Supervisors are responsible for ensuring that basic procedures are followed. Procedures may be bypassed only with the combined consent of the line manager, HR security officer and, where appropriate, the data protection officer (DPO). A written record of such decisions must be kept.
-

- Employees of all grades are permitted access only to those parts of the computer system which they need to enter in order to carry out their normal duties. Levels of access will be decided by line managers in conjunction with the HR officer who will ensure that levels of access are consistent throughout Heydays Care and Support Services.

- Employees may access the internet but access to certain sites will be blocked. It will be a disciplinary offence to try to bypass such restrictions.

- All incoming emails will be monitored and scanned for viruses before being released to the recipient.

- Employees with access to personal data are in a particularly sensitive position and must bear in mind at all times the provisions of the DPA and the GDPR with regard to security. This is especially the case where the information relates to children.

- Passwords must be used at all times and changed regularly. Employees should not select obvious passwords but should ensure that they are of at least eight characters including numbers, letters, upper and lower case and at least one symbol. All passwords must be kept confidential. Employees must not give their passwords to other members of staff or to any person outside the organisation. Password-protected sites should be closed when finished with and computers switched off. Computers should not be left open and unattended.

- When an employee leaves the organisation or moves to a different department all passwords in that department will be changed. When an employee is given a temporary password to a higher level of access than he or she normally uses, that password must be cancelled after the individual ceases to need it.

- Supervisors are responsible for stipulating requirement for back-up operations in their own departments. Regular back up must be carried out in accordance with departmental instructions.

- All Heydays Care and Support Services software must be formally authorised by the HR officer. Regular checks will be made for viruses by the IT department.
- No external software may be used without authorisation by either the HR officer and the employee's line manager.
- No private work or computer game playing is permitted.
- The safekeeping of CDs and DVDs sent from external sources is the responsibility of the person to whom it was sent. All such CDs and DVDs must be checked for viruses by the IT department before use. CDs and DVDs generated internally must be kept in a secure place. Employees should be reminded that the Information Commissioner's Office (ICO) has imposed heavy fines on organisations after the loss of CDs and DVDs containing sensitive personal data.
- Misuse of computers is a serious disciplinary offence. The following are examples of misuse:

  a. fraud and theft

  b. system sabotage

  c. introduction of viruses, etc

  d. using unauthorised software

  e. obtaining unauthorised access

  f. using the system for private work or game playing

  g. breaches of the DPA and the GDPR

  h. sending abusive, rude or defamatory messages or statements about people or organisations, or posting such messages or statements on any websites or via email

  i. attempting to access prohibited sites on the internet

  j. hacking

  k. breach of Heydays Care and Support Services security procedures.

This list is not exhaustive. Depending on the circumstances of each case, misuse of the computer system may be considered gross misconduct. Please refer to the disciplinary rules and procedures. Misuse amounting to criminal conduct may be reported to the police.

- Management, in consultation with specialist auditors, may institute confidential control techniques and safeguards. Financial systems are subject to special reconciliation processes.
- All breaches of computer security must be referred to the relevant director or to the managing director. Where a criminal offence may have been committed, the board will decide whether to involve the police. Serious breaches must be reported to the ICO within 72 hours. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must be informed by a senior member of staff without undue delay.
- Any member of staff who suspects that a fellow employee (of whatever seniority) is abusing the computer system may speak in confidence to the HR manager.
- This policy does not form part of the contract of employment and any or all of its terms may be amended from time to time.