Security Policy

Information Technology (IT) Security Policy

Introduction

This policy defines a framework by which Charlton Athletic Community Trust (CACT) computer systems, assets, infrastructure and computing environment will be protected from threats whether internal, external, deliberate or accidental, covering all aspects of physical and information security.

Statement

This policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers, agency workers and anyone who has access to our IT and communication systems.

The General Data Protection Regulations (GDPR) (EU) 2016 and the Data Protection Act 2018 (DPA) places an obligation on organisations that process personal data. This is not a new requirement but has been specifically updated to focus on the types of controls in place to identify information risks. This exercise provides assurance that the appropriate security measures have been applied to protect the personal data that we collect, store and process. The measures must ensure the confidentiality, integrity and the availability of the systems and services and the data we process within them

Access to CACT's systems and information by all staff, contractors, sub-contractors, suppliers, is diligently monitored with the appropriate pre- security checks including contractual agreements that sets out the minimum security requirements for confidentiality, integrity, availability and accountability of CACT's information and systems.

Misuse of IT and communications systems can damage the business and our reputation. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Key Principles

- Staff are responsible for the security of any computer terminal used by them. Staff should lock terminals or log off when leaving items unattended or on leaving the office, to prevent unauthorised users accessing the system in their absence.
- If issued with a laptop, tablet computer, smartphone or other mobile device, it is to be kept secure at all times, especially when travelling. Never leave in cars overnight.
- Staff should not attempt to change, delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).
- When using CACT equipment away from the workplace, for example at home, staff must protect documents from being read by third parties and should access documents via SharePoint.

- Staff are required to familiarise themselves with this policy and related policies, to adhere and comply with requirements. Failure to do so may result in disciplinary action up to and including dismissal.
- As a minimum training requirement, all CACT staff are to complete Data Protection and Information Processing and Sharing through on-line modules.
- Heads of Department and line managers are responsible to ensure the implementation and compliance with this policy.
- Staff MUST report breaches of data security, or "near misses" to their line manager and the Head of Governance and Support Services as a matter of urgency.
- ITRM (CACT's IT Provider) manages, maintains and operates CACT's IT systems, core network switches, edge network switches, backup systems, and the overall network infrastructure interconnecting systems.
- CACT reserves the right to monitor, log, collect and analyse the content of all transmissions on networks and devices at any time deemed necessary for performance, fault diagnostic and compliance purposes.
- Personal devices not issued by CACT are not permitted to be connected to access CACT systems or data.

Physical Security Access:

- All CACT offices are access controlled at the point of entry by lockable or key pad controlled access.
- Staff sign in and out of office locations and must wear staff ID passes at all times.
- Visitors must sign in and out, wear Visitors ID badges and be accompanied by a member of staff in office areas.
- Locking-up procedures are in place at CACT locations,
- Access to secure IT Rooms within CACT's head office is limited to key personnel only for purposes associated with their role
- Access controls are in place for manual storage of Personnel files and personal data on participants that are stored in locked filing cabinets.
- Access levels to electronic filing is controlled by permissions and profiles.
- Portable IT equipment, for example, lap tops or iPads when not being used should be stored securely at all times for example locked in a desk drawer

Staff Leavers:

- Line mangers are responsible to ensure IT equipment and devices are returned to the HR Co-ordinator, (following CACT's employee leaving procedures).
- Email accounts and access to CACT's IT system are to be disconnected on employees' last working day.

Safe Disposal of Data:

- Disposal of IT equipment is undertaken by a registered third party complying with WEEE (waste electrical and electronic equipment) conditions. Please contact the Health and Safety Officer if you have any IT equipment to be disposed of.
- All personal printed documents and files must be shredded. Shredding machines are located at all CACT offices. Personal information must never be thrown away in in everyday rubbish or recycling.
- Safe disposal and destruction of data is detailed in the CACT Records Management Policy

Data Security

- Laptops, desk tops, mobile phones and other devices are registered to individual staff members of staff.
- All devices must be password protected and passwords updated every 60 days in line with guidance below.

Passwords:

Passwords must

- Passwords must not contain the users name or parts of the user's full name that exceeds two consecutive characters.
- Be at least eight characters in length
- Contain characters from three of the following four categories:

  English uppercase characters (A through Z)

  English lowercase characters (a through z)

  Base 10 digits (0 through 9)

  Non-alphabetic characters (for example,!,$,#, %)

Users will be prompted when their current password is due to expire. Complexity requirements will be enforced when passwords are changed or created.

Anti-Virus and Malware:

- Antivirus software protection is enabled across all devices. Windows security updates are installed automatically on log-in.
- Screen savers are posted after 2 minutes of inactivity.
- ITRM may disconnect a device from the network behaving abnormally due to a possible virus infection until deemed safe.
- Suspect phishing emails or other abnormalities must be reported to ITRM Service desk.

Remote Access:

- Remote access is available through Office 365, via SharePoint. Staff are required to use this at all times.
- Personal information must not be transferred from the network using portable storage devices, for example, memory stick, DVD, external hard drive, etc.

- External portable storage device use is **strongly discouraged** except for storing of non-confidential information for example, generic power point presentations or training materials. If use of a portable storage device is required for other purposes, authority must be given by a line manager and Head of Governance and Support Services.

Email:

- Symantec Cloud email filtering and content scanning is configured to minimise unsolicited correspondence and ensure the system is used appropriately.
- Automated scans to monitor and reduce spam, viruses and inappropriate content are regularly run**.**
- Do not open emails or links that appear suspicious. If you click on a link by mistake inform ITRM Service Desk immediately.
- Only send level of information required and to those that need it.
- Check email addresses are correct and consider necessity to cc people into the email
- If emailing confidential information, password protect the document and send the password in a separate email, by phone or text, or share documents vis SharePoint which is safer.

Internet and Social Media:

- Do not access any web page or download any image, document or other file which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral.
- Except as authorised in the proper performance of your duties, you should not under any circumstances use CACT systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki

Loss or Theft of Personal Information (Data Breach)

- All incidences of loss or theft of personal or confidential information must be reported to your line manager and the Head of Governance and Support Services as soon as possible, as the breach may need to be reported to the ICO within 72 hours. A written report/ email should be submitted containing:
    - Details of incident
    - Date of discovery of incident
    - Place of incident
    - Who discovered the incident
    - Action taken to mitigate risk to organisation
    - Any further action taken by the person discovering the incident at the time of discovery
- All breaches are recorded and actioned as appropriate. An investigation will be instigated and a decision taken whether the breach needs to be reported to a regulatory body or other third party, e.g. insurers, Information Commissioners Office, Charity Commission etc.

- A central register of all incidents including "near miss" breaches is maintained by the Head of Governance and Support Services and reviewed by the Information Governance Steering Group quarterly.

Responsibilities:

CACT's Board of Trustees will approve the IT Security Policy and is also responsible for ensuring that sufficient resources are provided to support the requirements of this policy and related policies.

The Information Governance Steering Group, comprises the CEO, Executive Team, and members of the Senior management Team, Representing all strands, is responsible for overseeing all aspects of Information Governance; developing and maintaining all related policies, standards, procedures and guidance, training and raising awareness of best practice. Meetings of the Information Steering Group are scheduled annually and take place quarterly, with additional meetings if required. The Board of Trustees received and discuss minutes of the meetings at their quarterly Board meetings.

Managers within CACT are responsible for ensuring that the IT Security Policy and other related policies and guidelines are built into local processes and that there is on-going compliance.

Staff are responsible for ensuring that they are aware and understand the requirements of the policy and for ensuring compliance on a day-to-day basis.

CACT acknowledge that information is a valuable asset and will ensure that the information it holds, in whatever form, is appropriately managed and stored to protect the interests of all stakeholders.

Policy review

The policy will be reviewed and approved by the Board of Trustees on an annual basis or sooner if required e.g. where there are changes in legislation, or recommended changes to improve best practice.

Drafted March 2017 **Approved: March 2017**
Review: March 2018 **Approved: June 2018** (updated to reflect GDPR requirements)
Reviewed: June 2019 **Approved: July 2019**
Next Review June 2020

Related Documents:

CACT Information Governance Policy
CACT Data Protection Policy
CACT Information Sharing Policy
CACT Records Retention Policy
Clear Desk Guidance