IT Security Policy

Introduction

East Birmingham Community Forum Ltd

IT Policy

This IT policy is provided as a central reference for all managers, supervisors, leaners and employees and applies to staff across all locations where East Birmingham Community Forum Ltd (EBCF) carries out its work.

The specific policies that follow promote the philosophy of East Birmingham Community Forum Ltd regarding standards of excellence; terms of employment; employee development; and employee services.

It may be necessary to change these policies from time to time to reflect changes in the workforce, employment trends, economic conditions and UK and European legislation. However, any changes in policy will be consistent with EBCF's approach to:

- Communicating EBCF's standards and expectations in all aspects of employment including performance.
- Valuing diversity and assure equal employment opportunity and a workplace where relationships are based on mutual respect.
- Treating all staff, workers, contractors, learners and customers in a professional, non-discriminatory manner.
- Providing safe, effective working conditions.
- Providing competitive terms and conditions in our workplace market.

Any policy/procedure changes will be fully consulted on and communicated to all staff through normal communication channels. This IT policy manual will be updated annually.

This IT policy manual should be read in conjunction with EBCF's Staff/Learner Handbook and HR policies and procedures manual.

Contents

IT Security Standards Policy

This document is a summary of the IT Security Standards EBCF must adopt and comply with at all times.

For all employees

It is the responsibility of the company IT department to maintain security of its devices and services. You must not intentionally or negligently disable or bypass security measures or attempt to do so. You are not expected to know all of these Security Standards, however if you become aware or suspect that a device or service the company uses does not comply, you must inform IT immediately. Any employee who has a non-compliance with these standards will be referred to the disciplinary policy and referred to HR.

With the company's transition to Azure Cloud services (Nov 2023), the IT department no longer performs local backups. Instead, employees are solely responsible for backing up their data using their company OneDrive accounts., as mentioned in the Backup Policy. You may only back up your data to a device or service that also meets the Security Standards. Your @ebcf.org.uk OneDrive account does.

For "system owners"

Every device, system, or service the company subscribes to and uses is considered to have a system owner or joint system owners. The system owner(s) is responsible for ensuring compliance with the Security Standards, as well as for handling administrative access in accordance with the Administrator Accounts Policy.

Note that some devices may fall into more than one of the categories below, for example a VM hosting multiple services.

In most cases the system owner is a member of IT staff, but this is not always the case. For example, some systems must be controlled by directors or senior management.

In the event of a conflict between requirements from two sources, the decision as to which prevails must be made by directors or senior management.

For items listed as "strict compliance", all requirements must be met, and the company must provide the resources to do so. However, the IT Security Standards are concerned only with designed behaviour. Cyber Essentials requires that available security patches must be installed, but the presence of vulnerabilities and exploits whether known or unknown that do not have a patch or feasible mitigation available does not constitute a breach of these standards.

For items listed as "reasonable efforts", they should be implemented "by default" but may be deviated from if there is a clear business need or due to budgetary constraints.

All devices, systems, and services.

Cyber Essentials: Requirements for IT infrastructure, v3.2, https://www.ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-2.pdf. Strict compliance.

Devices, systems, and services must be configured with an appropriate form of central management. This must enable the system owner to monitor and make changes to devices or accounts (as appropriate) without the intervention of or disruption to their end users. For portable devices this

must function whenever the device is connected to the internet without requiring further user intervention and must include some method to remotely wipe data on the device. Strict compliance.

Standard users must be prevented from running unauthorised software, apps, add-ons, plugins, or any similar thing, including software etc that runs without “installation”. This applies to cloud services and systems as well as to physical devices. Strict compliance.

Security settings must be locked down so that users cannot modify or disable them. Strict compliance.

Windows PCs.

NCSC End User Device Security Guidance, https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides/windows . Reasonable efforts.

Windows Security Baselines, https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines . Reasonable efforts.

Devices must automatically lock after 2 minutes of inactivity or less. Strict compliance.

BitLocker encryption must be enabled for all internal drives and configured to use an AES-256 bit encryption method. TPM unlock is acceptable. The BitLocker recovery password must be stored in EBCF’s Active Directory and in no other location. Strict compliance.

SMBv1 and SMBv2 support must be disabled, for both client and server functionality. SMBv3 must be configured to require encryption. Strict compliance.

Android devices.

NCSC End User Device Security Guidance, https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides/android . Reasonable efforts.

Devices must automatically lock after 2 minutes of inactivity or less. Strict compliance.

Encryption must be enabled for device storage and must use an AES-256 bit encryption method. Any recovery keys or passwords must be treated as CONFIDENTIAL and stored accordingly. Strict compliance.

iOS devices.

NCSC End User Device Security Guidance, https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides/ios-and-ipados . Reasonable efforts.

Devices must automatically lock after 2 minutes of inactivity or less. Strict compliance.

Encryption must be enabled for device storage, and must use an AES-256 bit encryption method. Any recovery keys or passwords must be treated as CONFIDENTIAL and stored accordingly. Strict compliance.

Linux physical servers (including hypervisors).

All storage must be encrypted using LUKS with an AES-256 bit encryption method. TPM unlock is acceptable. An unlock passphrase must be set and a copy printed out, classified CONFIDENTIAL, and stored securely by the EBCF directors. Strict compliance.

User Access Controls Policy

1. Objective

User access control (UAC) is used to ensure that only authorised users are able to gain access to sensitive information and locations. By ensuring that only authorised individuals have user accounts, and that they are granted only as much access as they need to perform their role, the company can reduce the risk of information being stolen or damaged.

Compared to normal user accounts, accounts with special access privileges have enhanced access to devices, applications and information. When such accounts are compromised, their greater freedoms can be exploited to facilitate large-scale corruption of information, disruption to business processes and unauthorised access to other devices in the organisation.

If a user opens a malicious URL or attachment, any associated malware is typically executed with the privilege level of the account that user is currently operating. Therefore, the company must take special care over the allocation and use of privileged accounts. Ideally, UAC ensures that all users have only those rights and access privileges which they require to perform their day-to-day tasks, and no more. This is known as the "principle of least privilege". Where additional rights and privileges are necessary to perform a specific task, temporary escalation can be granted.

2. Scope

The scope of the policy covers all individuals either employed or contracted to work with or for the company, either in-office or remotely.

3. Policy

The company uses the following types of accounts:

- employee accounts, which are granted only those rights and access privileges that the individual user requires to perform their day-to-day job;
- contractor accounts, which are granted temporary rights and access privileges on a per-request basis;
- customer accounts, which are granted only those rights and access privileges that the individual user requires to access the services the company provides;
- customer accounts by external SSO, which are granted only those rights and access privileges that the individual user requires to access the services the company provides, and for which authentication is handled by the SSO provider and the company does not store or control the credentials;
- administrator accounts, which are given increased rights and privileges and can only be accessed from employee accounts with rights to do so, and only with authentication. The Administrator Accounts Policy details how these accounts are defined and how they must and must not be used.

All types of account are subject to the following rules:

- As per the staff approval process, Line managers must request in writing the level of access needed for their staff member to do their day to day job.
- If there is a change in job role, the line manager must inform HR and the IT department to get the required access increased in line with their job role.
- Leavers from the company – the line manager of the member of staff MUST inform the IT department within 2 hours of the person leaving. IT department with then suspend / remove access to all company assets. Emails will be immediately redirected to the line manager until further notice.
- All employees, contractors, and customers must be allocated a unique identifier.
- Sharing accounts between multiple people is prohibited. This includes but is not limited to sharing passwords, registering multiple people's biometrics to a single account (for example for unlocking a smartphone), and logging in then letting someone else use the computer.
- All account usage is subject to monitoring by EBCF IT staff.

If you require a temporary escalation of privileges, contact IT. Information classification (see the "Information Classification & Protection Policy") is enforced, where possible, by UAC, as is the tracking and attribution of modifications.

Administrator Accounts Policy

What is an Administrator Account?

With some systems and services, especially SaaS (cloud) services, things are more complicated than just user versus administrator. No definition can cover every possible scenario and system owners (see below) are expected to use good judgement.

In general an account is an admin if it can manage other user accounts, access other users' data bypassing normal controls, or controls infrastructure that other systems rely on (for example DNS).

Some cloud services offer only one level of user privileges. In that case the accounts should *probably* be considered admins.

Using admin access

All persons using any admin access must read and understand this section first.

The use of admin accounts creates additional risk. Malware can do far more damage if it is able to run under an admin account, therefore you must follow this policy to avoid that risk.

You must:

- Use admin access only for the tasks that you are authorized to do and that require admin.
- Not use admin access on devices for web browsing or email. If you need to download a file, do that using your normal account then transfer the file via network or USB.
- Not use admin access to cloud services routinely.
- Ensure you log out from cloud admin accounts promptly after finishing administrative work. Private/Incognito browsing is suggested.
- Never share your admin login with anybody else.
- If you have multiple admin accounts, use the one with the least privilege required. For example do not use a Domain Administrator account for a task that only requires local Administrator on the PC.

The way you use your admin account will vary depending on the system and task. When you are granted admin access you will be told and must understand the method favoured. Examples include:

- Admin in a virtual machine. The favoured method for admin on devices, ensuring your admin access is in a contained environment separated from other company data.
- Run As / UAC / sudo. The usual method to run a program that needs to make changes to your main computer, such as a software installer.
- Direct login. Sometimes required for programs and setting changes that do not work with Run as.
- Temporary promotion of your normal account. If this method is used, you will complete the tasks only under supervision and must not do any web browsing or email until your account is demoted again. It is rare that this approach will be required.
- Use of a Privileged Access Workstation to administer critical cloud services in a maximum-security environment.

Granting and reviewing admin access

Admin accounts on computer systems must be granted only when necessary for an employee or outside partner to do their work. Consider if there is a reasonable alternative.

Admin access must be granted in accordance with the principle of least privilege, being given only the rights and permissions needed for the user to perform the admin tasks required for their job role, and only on the systems required. For users who have a wide range of admin tasks to perform such as IT staff, consider giving the user multiple accounts so that routine lower-risk tasks (eg installing software) are not carried out with accounts that have higher-risk rarely-needed privileges (eg full Domain Admin).

Every system must have one or more defined 'owners', who have the authority to grant admin access to others. The system owner is responsible for evaluating if admin access is truly required. They must also document any admin access and must set a reminder in their calendar or diary to review the grantee's need for continued access. The reminder date may be chosen as appropriate but must in any event be within the next year.

The grantee must understand the policy above, and what tasks they may (and may not) use their admin access for and how to do them. The policy above lists some methods but others may be used.

Sharing the same admin login between multiple people must not be done under any circumstances. Cyber Essentials permits no justification or exception for admin account sharing. It is permissible for a system owner to **transfer** use of an admin account from one person to another if required; this is intended for systems that do not support multiple admin accounts. The date and time of the transfer, in both real time and the system's time (in case of any discrepancy), must be documented and credentials changed immediately so the old user no longer has access.

If the grantee changes job role, their admin access must be reviewed promptly.

Backup Policy

1. Objective

This policy is designed to protect the company against loss of data. This policy is also designed to ensure that the organisation can protect its data and ensure that they can be recovered in the event of equipment failure, intentional/accidental deletion or destruction due to fire, flood or any other such disaster. It is not the intention of this policy to ensure the quick recovery of files that may have been deleted in error or updated incorrectly by the user. The restoration of such files may only be considered if they are required to fulfil a legal, contractual or regulatory obligation or a pressing business need. Should computer systems become infected with malicious code (such as ransomware that encrypts data and requires payment to the criminal in order for the data to be unlocked) or a severe incident such as fire or flood occur, restoring from a successful backup will be the only way that the company may continue to do business.

2. Scope

The scope of the policy covers all individuals either employed or contracted to work with or for the company, either in-office or remotely. It covers all information handled by the company, whether in digital or physical (e.g. paper) form.

3. Policy

The company processes a wide variety of information.

3.1 Data Protection

The information classification (as defined in the “Information Classification Policy”) is taken into consideration when backing up the data so that it is given the relevant level of protection during its entire lifetime (i.e. from its creation until its archiving and destruction). It must be secure when stored and transported.

Information that pertains to any identifiable living human is protected in line with the Data Protection Act 2018 and the EU General Data Protection Regulation — specifically, it is not stored for longer than there is a business need. Such information is also stored in an encrypted format and only ever within the European Economic Area.

Encryption keys are stored in line with the “Information Classification and Protection Policy”.

3.2 Frequency and retention of backups

With the company's transition to Azure Cloud services, the IT department no longer performs local backups. Instead, employees are responsible for ensuring business data is stored within approved company systems, such as OneDrive or SharePoint, which provide centrally managed backup and recovery capabilities. This ensures an additional level of protection. Remember, a file is only backed up if there is a copy in two or more places.

Data on desktop PCs, laptops, and servers should be backed up to OneDrive to ensure data integrity. Employees must ensure that their important files are regularly synchronized with OneDrive.

Backups are performed continuously via OneDrive's synchronization feature, ensuring that the most recent version of files is always available. Data stored in OneDrive is protected against malware, including ransomware, by leveraging Azure's security features.

Data is retained in OneDrive based on business needs and regulatory requirements. Employees must manage their data according to these guidelines to ensure compliance.

3.3 External Services

Staff are not permitted to use accounts other than those authorised by the company. In any instance where such use is required, express and documented permission must be obtained from senior management authorising such an arrangement. A log of those arrangements will be maintained by senior management.

The company loses the control of its information if users set-up such accounts without authorisation. Though these services offer the ability to store files off-site for safe keeping, it may be the case that the company is breaking contractual or regulatory obligations by storing information on these platforms.

Section 3.4 intentionally omitted.

3.5 Verification

Data protection and recovery capability is primarily provided through approved cloud services, including Microsoft OneDrive and SharePoint, which include built-in versioning, recycling, and recovery features.

To ensure that recovery functionality remains effective, periodic restore tests must be carried out. These tests may be performed by IT or by designated system owners or users under IT guidance.

Verification activities must include:

- confirmation that files can be restored using OneDrive/SharePoint version history or recycle bin functionality;
- periodic user-level restoration testing of randomly selected files or folders;
- confirmation that restored data is accessible, intact, and reflects expected versions; and
- validation that users are correctly storing business data within approved systems.

The frequency of verification must be determined by IT and should be no less than annually, or more frequently where required by business or compliance needs.

Any failures in restoration or data recovery must be reported to IT and investigated as an information incident.

Evidence of verification activities must be retained for audit and compliance purposes.

Communications Policy

1. Objective

The company encourages the use of electronic communications media, such as email, social media and text messaging, where it supports the organisation's goals and objectives. The purpose of this policy is to ensure that where used, electronic methods of communication are protected to prevent loss of data and reputational harm to the company or its employees.

It is important that employees understand the limitations of the use of electronic communication media and the potential risks they can bring to the company. For example, sending personal information to the wrong individual(s) could breach regulations on data privacy and could lead to the company being fined heavily by the Information Commissioner's Office.

Electronic communication media, especially email, are also a common method of attack for criminals to try to infect computer systems with malicious code or mislead employees into revealing sensitive information.

2. Scope

The scope of the policy covers all individuals either employed or contracted to work with or for the company, either in-office or remotely.

3. Policy

Staff must remain vigilant of potential scams or other fraudulent activity in line with the company's "Social Engineering Policy".

Each employee may only use the company email system if they:

- comply with current legislation;
- use electronic communications in an acceptable way (see below)
- do not create unnecessary risk(s) to the company by their misuse of any electronic communications system(s). Company electronic communications shall only be sent using company sanctioned devices and services to ensure that they:
    - are up to date with the latest security patches
    - have a sufficient level of anti-malware protection in place
    - have a firewall that is configured correctly. In addition, the company reserves the right to view the contents of any work-related electronic communications account without notice to ensure that procedures are being followed.

3.1 Acceptable use of company electronic communications media

- As each user is representing the organisation, it is important that only messages containing true information are sent.
- Any electronic communication(s) received that is found to contain inappropriate material (which could be deemed illegal, obscene, hateful or commonly thought of as being objectionable and offensive) must be reported to a line manager.
- Each electronic communication must only go to the intended recipient(s) – care shall be taken to ensure that “auto-complete” services do not insert the wrong name of the recipient(s).
- Electronic communication(s) must only be sent to people that have authority to view it; when sending to groups, employees must ensure that all members of that group have authority to see that electronic communication(s).
- Users shall only send electronic communications if they contain, or request, work-related material. All information sent in electronic communications must be true to the best of the employee’s knowledge.
- The content of the electronic communication sent or received must be handled in accordance with the "Information Classification & Protection Policy", which states when encryption is required, how electronic communications must be handled across all points of their life cycle and the types of content that are forbidden in electronic communications, even in draft form.
- Users that receive spam or suspected fraudulent electronic communication(s) must inform IT.
- Each electronic communication sent must contain a disclaimer that has been agreed by senior management.
- Users are responsible for all communications that originate from personally owned accounts. Ensure that they are secured in line with the “Passwords & Authentication Policy” and are not left accessible at your workstation in line with the “Clear Desk Policy”.
- Use of web-based email may only be through company-owned devices.
- Create electronic communication service accounts protected by secure authentication methods, as described in the company’s “Passwords & Authentication Policy”.
- Users are responsible for archiving or deleting electronic communications more than 1 month old.
- Always encrypt sensitive attachments before sending.

3.2 Unacceptable use of electronic communications media

Employees shall never:

- take actions that may introduce any form of computer virus or malware into the corporate network by:
    - clicking on attachments or hyperlinks within electronic communications that were from unknown senders or otherwise unexpected;
    - disabling or re-configuring the security software on the device.
- send electronic communications that may bring the company into disrepute;
- sending work-related emails from a non-work electronic communication account;
- use the company electronic communication system(s) for personal business or non-company purposes;
- forward electronic communications classified as anything other than PUBLIC to external locations;
- send electronic communications which have an excessively large file size;
- distribute or store information deemed illegal, obscene, hateful or commonly thought of as being objectionable and offensive;
- distribute or store details considered discriminatory, offensive or abusive. Electronic communication must not contain sexist, racist or otherwise discriminatory remarks, information that could be taken as a personal attack or could be considered as harassment;
- disseminate information in a way that violates copyright law;
- make unauthorised use of another user's electronic communications media account;
- send unsolicited advertising material;
- open spam, even to unsubscribe or ask for no more communications. Staff shall delete the electronic communication after blocking the sender via the tools found in their electronic communication client;
- send sensitive attachments 'in the clear'.

3.3 Non-company use of electronic communications media

Though employees will likely have personal electronic communications media accounts, such as personal email accounts or social media profiles, they should bear in mind that their actions and views expressed on such platforms may still be construed as reflecting the views of their employer. They are therefore asked to keep the previous guidelines in mind even when using non-company-owned electronic communications media.

In addition, employees are asked to be careful about work-related and personal information that they post online. This can prove useful to malicious attackers through Social Engineering — see the "Social Engineering Policy" for more.

Disposal and Destruction Policy

1. Objective

This policy governs the secure disposal of company information according to its classification, the criteria for which are given in the “Information Classification & Protection Policy”.

For the purposes of this policy, the term “sensitive information” includes any information covered by contractual, legal or regulatory obligations or that which could damage the company’s reputation or ability to trade if disclosed or lost. As per the “Information Classification & Protection Policy”, all information classified as anything other than PUBLIC is considered sensitive.

2. Policy

All sensitive data is retained according to business, legal, regulatory and contractual requirements as defined by owner of the information. When there is no longer a justified requirement for the storage of the information, then it is disposed of securely.

2.1 Re-use of Devices and Storage Media

Devices may only be reused within the organisation and may not be sold on, or otherwise used for non-company matters, unless the information has been deleted securely by a “wiping” utility approved by the Head of IT. Depending upon the sensitivity of the information, the company may not allow devices to be re-used outside of the company.

2.2 Disposal and Destruction

All sensitive information must be disposed of using methods that meet BS EN 15713:2009, and for electronic media and equipment also meet the NCSC guidance on secure sanitisation of storage media, https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media This requirement includes all information stored in a digital form, whether it be stored in the memory of a photocopier, printer, workstation, laptop, mobile device, removable storage media, or other device, or in a temporary file, as well as any information stored in a non-digital form, such as on paper.

Shredding devices must cross-cut the paper (P-4 rating or better) to ensure the documents cannot be reconstructed. If documents cannot be shredded immediately, then the documents must be stored in secure bins until shredded. Where a disposal company is used, a certificate of destruction must be issued.

Depending on the sensitivity of the information, the company may not allow devices or storage media (including paper) to be disposed of off-site. In this instance the contracted company must crush/wipe the devices on the premises.

Information Classification Policy

1. Objective

Information is classified so that appropriate levels of protection can be applied to the way in which the company handles information, from its inception to its destruction. A number of different factors have to be considered before information can be appropriately classified – this includes a consideration of any legal requirements, service level agreements, values, sensitivity of the document to unauthorised disclosure etc.

So that information is seen, changed or destroyed only by those authorised to do so, the company classifies its information. Staff must handle information in line with the requirements of its classification.

The level of classification afforded to information is based upon the level of confidentiality, integrity and availability of the same.

This policy also governs the appropriate use of cryptographic controls (encryption methods) to protect information against accidental or malicious disclosure and to ensure the confidentiality, integrity and availability of any information.

2. Scope

The scope of the policy covers all individuals either employed or contracted to work with or for the company, either in-office or remotely.

3. Policy

As of July 2022 the company is not enforcing classification of all documents and information. Classification is at the discretion of the document creator.

The company uses 4 classifications, and where information may not be labelled, it is up to each individual to recognise the class of information they are handling and deal with it accordingly. Information not classified should be treated as INTERNAL or higher unless it is very obviously PUBLIC. Fewer people will be involved in processing and handling the information as its classification increases.

The company protects its sensitive information, that of its third parties, customers, clients and stakeholders, by the use of cryptographic controls wherever there is a legal, regulatory or contractual obligation to do so, or when the disclosure of such information could cause damage to the cash flow or reputation of the company. Encryption extends from the creation of a piece of information, through any use or transit, up until its destruction (as per the “Disposal & Destruction Policy”).

Company information will always fall into one of the following classifications:

3.1 Information Classifications

1. PUBLIC – In general, this is business information that is not subject to special protection and may be routinely shared with anyone inside or outside of the business. Such information can be made public with no impact on the business or may already be in the public domain.

2. INTERNAL – Information such as internal policy documents, general company minutes of meetings, procedures and work instructions that are only of relevance to staff members generally fall into this classification. Access by third parties must be authorised by senior management. Think of this as information that should be kept within the company and not shared publicly. Should it be made available outside of the company to unauthorised persons, there may be a negative impact to the business

3. RESTRICTED – This information is sensitive in nature and access is restricted to senior management. Authorisation for other employees or third parties to access this information must be granted by senior management. Such information is often either protected by statutes, regulations, contract or company policy. Examples include client records, personal information, financial documents and any other information that may cause reputational damage, harm, distress or embarrassment to the individuals or companies involved if the information got into the public domain.

4. CONFIDENTIAL – This information is highly sensitive in nature and generally includes company details that could cause high impact to the business should it be disclosed to competitors or members of the public. It includes company secrets, inventions and strategies and is restricted to directors. Authorisation can only be granted by directors when other employees have a 'need to know'. Access by third parties must be authorised by directors.

Sections 3.2 and 3.3 intentionally omitted.

3.4 Disposal or Re-use

Secure disposal, destruction or reuse of data and equipment must be done in accordance with the company's "Disposal & Destruction Policy". RESTRICTED information must be destroyed personally by senior management, or by a third party contractor with contractual guarantees of confidentiality and all industry standard accreditations. CONFIDENTIAL information must be destroyed personally by directors, or by a third party contractor with contractual guarantees of confidentiality and all industry standard accreditations.

3.5 Removal of Property

The following may only be taken off-site with the permission of senior management:

- Personnel files
- Client information

- Laptops (unless already allocated to the individual)
- Mobile phones (unless already allocated to the individual).

Care must be taken at all times to ensure the security of such assets and they must not be left unattended away from the office or home.

The information stored on the assets must be done in accordance with the handling procedures and information classification stated in this policy.
Depending on the sensitivity of the information, the company may not allow devices or storage media (including paper) to be disposed of off-site. In this instance, the contracted company must crush/wipe the devices on the premises.

3.6 Encryption and Classification

Approved secure authentication methods are defined in the company's "Passwords & Authentication Policy". Approved secure methods of connecting to public Wi-Fi networks are covered in the "Public Wi-Fi Policy" and approved secure methods of transmitting information across the Internet are detailed in the "Internet Usage Policy".

RESTRICTED and CONFIDENTIAL information may only be stored on servers, workstations or laptop drives that are encrypted, or in a cloud storage service approved by IT.

Similarly, any transmission of RESTRICTED or CONFIDENTIAL information across public networks (i.e. the Internet) or storage on removable media must also be encrypted.

3.7 Data Sent Outside of the UK

If data is to be sent outside of UK, it is the responsibility of the user to check to ensure that they are abiding by international cryptographic and data protection legislation.

3.8 Management of Cryptographic Keys

All cryptographic keys/certificates for servers administered by the IT department are stored centrally in a password vault with restricted access.

Internet Usage Policy

1. Objective

The company has a strict policy against unauthorised or inappropriate use of Internet services or content. This is to protect the company against malicious attacks and unauthorised access to sensitive information.

It is to be remembered that information found on the internet cannot always be trusted, and therefore may only be used for business purposes after its authenticity and correctness has been verified.

Employees must remain vigilant of potential scams and other fraudulent activity in line with the company's "Social Engineering Policy".

Internet access may be monitored for network management, or security purposes. Bandwidth usage and time restrictions may be applied where necessary.

Web browsing is a common method of attack for criminals to try to infect computer systems with malicious code or mislead employees into revealing sensitive information.

2. Scope

The scope of the policy covers all individuals either employed or contracted to work with or for the company, either in-office or remotely. It also covers connections to the Internet made from any Internet-enabled devices, from workstations to mobile devices.

3. Policy

When using company devices, users may only access the Internet via the company network where suitable firewall protection is deployed. Users shall not seek to bypass the company's firewall controls via mobile tethering, modems, Wi-Fi or other such direct access unless otherwise instructed or authorised by IT. Company devices are only used for Internet access if they have the following installed:

- Vendor-supported operating systems that are patched up to date;
- Up-to-date malware protection software paired with the latest virus definition files that are configured for on-access scanning of all files including those being downloaded from the Internet;
- Correctly configured personal firewalls, set to block unsolicited inbound traffic.

The company reserves the right to block access by individuals and/or groups to certain Internet services and Web pages where it deems it necessary. If access is required to such sites for work-related activity, then a written request shall be submitted to IT with the relevant authorisation of senior management. Under no circumstances must the user seek to circumvent the company's controls and browse unauthorised Web pages when using company equipment and/or company networks.

Users of company-owned laptops and mobile devices may only connect to the Internet in line with the “Remote Working Policy". Users of such equipment are responsible for responding to any system alerts and applying updates where necessary, or informing IT to help rectify any issues before continuing to use the system(s).

Users who are authorised to connect to the Internet from remote locations, and who are therefore not protected by the company’s firewalls, shall only visit Internet services and websites that relate to work activity.

Employees that post messages on social media, forums, etc. must unambiguously state that their messages do not represent the organisation's viewpoint. Users must advise IT when there is no longer a need to have an online account, to ensure that it is removed.

3.1 Unacceptable use or behaviour

Whilst using company equipment, the user shall not:

- visit Internet sites that contain illegal, obscene, hateful or other information commonly thought of as being objectionable and offensive;
- use company user IDs or email addresses when signing up to non-work-related services;
- use the same text-based authentication credentials on multiple online services;
- create business accounts on online services without authorisation from senior management or IT, regardless of whether these services require payment or not;
- upload company data to online services without authorisation;
- upload any information onto websites that may bring the company into disrepute;
- download, run or otherwise accept any software from the Internet unless part of an authorised procedure;
- seek to bypass or change the installed anti-malware protection software or any other security mechanism including personal firewall settings;
- browse the Internet whilst logged-in to the computer as an administrator of the device;
- place the company’s details, Web or electronic communications details on any site without prior authorisation as this could potentially bring the company’s reputation into disrepute.

As Internet traffic may be monitored for breach of policy, users must alert IT should they:

- inadvertently visit a suspicious website that they suspect contains malware and/or other harmful elements;
- inadvertently visit a website that contains illegal, obscene, hateful or other information commonly thought of as being objectionable and offensive.

IT Asset Procurement, Management, and Disposal Policy

This policy covers the procurement, management, and disposal of IT assets used by EBCF. It includes both physical assets and commercial software licenses. It does not apply to non-commercial software or to business data; these are addressed by other policies and documents such as the Approved Software Policy and the Personal Data Inventory.

Purchasing - General

The process for purchasing is as follows:

1. An employee in a management, supervisory, or IT role identifies a business need that is not being met by existing assets, and requests the new hardware or software from the IT department.
2. The IT department must first check that there isn't already suitable hardware or software available.
3. Once the need for a new purchase is agreed, the IT department must evaluate at least two options on the basis of TODO as well as compliance with any other relevant policies. The options shortlisted must be chosen in good faith.
4.
    a. If the cost of the asset is at petty cash level, a member of IT staff may immediately purchase the item following the process for petty cash expenses.
    b. If the cost of the asset is more, the IT department will request the Finance Director approve and make the purchase.
5. Once the asset is received, the IT department must take the delivery and ensure it is included on the relevant asset register. The IT department must then ensure the asset is correctly configured, if applicable, before deploying or issuing it for use by employees.

Moving assets

Windows desktops and peripherals may be moved within a single office by management if there is a business requirement. The IT department must be informed that this has been done. Users are advised that desktops moved may not correctly function until the IT department can configure the infrastructure.

Portable computing devices including laptops, tablets, and smartphones are covered by the Remote Working Policy; this applies to such devices even if they are not leaving the office.

No other assets may be moved, and no assets moved between offices, without the prior consent of the IT department.

When assets must be moved between different offices or transferred to a third party (eg for repair), appropriate insurance must be in place to cover damage or loss in transit.

Surveying assets

At least once a year a survey must be taken to ensure that the company still possesses all registered assets and is not using any unregistered assets. Discrepancies must be treated as IT incidents and investigated accordingly.

Disposal – General

IT assets may only be disposed of with authorisation by senior management. Assets that store data must be wiped in accordance with the Disposal and Destruction Policy. Assets for disposal must be labelled accordingly and stored securely until they are collected or transported by a waste carrier or purchaser.

Asset Registers

Where possible, assets should be configured with a management or monitoring tool which can automatically record serial numbers and similar information, avoiding error-prone manual entry. The list of asset registers must be maintained here.

Assets that store company data *must* be registered. Registration of assets that do not store data may be dispensed with if the value is too low to justify the overhead of registration.

- Mobile device management – Android and iOS devices.
- Microsoft 365 – Microsoft subscription software licenses.
- PDQ Inventory – Windows PCs.
- Unifi controller – Unifi network equipment.
- Volume Licensing Service Centre – Microsoft perpetual software licenses.
- VoIP management portal – Desk and cordless phones. Note that EBCF leases, not owns, this equipment.
- Not registered – Monitors, keyboards, mice, cables.
- IT Asset Register spreadsheet – Items not above mentioned, including servers and non-Unifi network equipment.

EBCF Password and Authentication Policy

Classification: INTERNAL

Last updated: 28 August 2022, MFA on MS365 is now rolled out. (reviewed on 12/08/24)

In accordance with the recent changes to Cyber Essentials the EBCF Password Policy applies to **all** computer systems and accounts you use for your work for EBCF and that use a password for login. It applies to all individuals employed or contracted to work with or for EBCF regardless of physical location.

Multi-factor authentication:

Multi-factor authentication **must be used where available**. This most commonly involves you receiving a code by text message after inputting your password. As of 28 July 2022 it is available for many cloud services including EBCF's Microsoft 365 (email, OneDrive, etc), but is not available for EBCF computer logins.

Passwords must be:

- **Changed by you** from any initial value to a password that complies with this policy.
- **Not shared with anyone.** All logins are for the use of only the person they are assigned to.
- **Unique to EBCF**. Do not use the same password for your work as you use for your personal email, Facebook, etc logins. It's very common for hackers to steal email addresses and passwords from an insecure website and use them to break into your account on other sites.
- **At least 8 characters.** Longer is better. (The computer normally won't let you use a shorter password). Administrator account passwords must be at least 12 characters.
- **Not a common word or phrase.** However three or more *random* words will make a strong password.
- **Not related to you, your family, or EBCF.** Or a hacker who knows you will guess it.
- **Stored securely or memorised.** You can store them using KeepassXC which is installed on our computers. If you write down a password make sure it's stored in a locked drawer or cabinet.

If you think someone knows your password who shouldn't or your account has been broken into, **change your password** and **inform IT staff or your manager.**

PINs and patterns:

A PIN or pattern that is used to log in to or unlock a device you have physical possession of, such as a mobile phone or laptop, has a reduced minimum length of **six** characters or points.

Biometrics:

Biometrics may be used instead of, or as well as, a password to log in to or unlock devices you have physical possession of, such as a mobile phone or laptop. Biometrics are not approved as the *only* factor for logging into a website or remote service and must be combined with another factor.

Public Wifi Policy

1. Objective

The company encourages work-related Internet and email use whilst not on company premises, as long as the devices used to achieve this have been sanctioned by the company. Using public Wi-Fi to conduct business, without the necessary safeguards, places our data at risk of theft.

2. Scope

The scope of the policy covers all individuals either employed or contracted to work with or for the company, either in-office or remotely.

3. Policy

Devices used on public Wi-Fi that are not sanctioned by the company include home PCs or public access PCs (i.e. those found in libraries, hotels or cafes). Though the company takes every effort to ensure that devices are adequately protected, it is the responsibility of the individual to ensure that, before connecting to the Wi-Fi network, the device has:

- up-to-date antivirus and antispyware software;
- a firewall that is activated and configured to company requirements (i.e. the settings have not been changed) since the device was issued;
- all software (including your Web browser) is current with automatic updating;
- file sharing is switched off.

4. VPN Usage

To further protect company data while using public Wi-Fi, employees and contractors must adhere to the following guidelines regarding the use of the company's Virtual Private Network (VPN):

- VPN Connection: Whenever accessing company resources (such as email, internal systems, or confidential files) over a public Wi-Fi network, employees and contractors are required to establish a secure VPN connection before transmitting any data. This ensures that all communications are encrypted and less vulnerable to interception.
- Approved VPN Software: Only VPN software that has been sanctioned and provided by the company should be used to connect to the company network. Use of third-party VPNs not approved by the company is strictly prohibited.
- Training and Setup: Employees and contractors will be provided training on VPN setup and use before they are allowed to access company resources via public Wi-

Fi. The IT department is responsible for establishing a secure connection, verifying its security, and troubleshooting common issues.

- Connection Integrity: While connected to the VPN, users must remain vigilant and ensure that their connection to the company network is active and secure throughout the session. Any disconnection from the VPN must be addressed immediately, and all data transmission must cease until a secure connection is re-established.

For security reasons staff must:

- not follow prompts to update software whilst connected to a public network;
- never connect to any public Wi-Fi network secured with WEP, WPA or WPA2—only WPA3 is to be used.
- never transmit any data that is deemed CONFIDENTIAL or RESTRICTED in line with the company's "Information Classification & Protection Policy", unless a secured VPN tunnel has been established and the user has been trained in setting up such a connection;
- ensure that URLs in Web browsers are actually pointing to the expected place in case a criminal has hijacked the Wireless Access Point and is forwarding traffic to their site;
- ensure the connection is encrypted wherever corporate data is transmitted (check that https:// appears in the address bar of the browser) even if the data is not classified as CONFIDENTIAL or RESTRICTED;
- ensure that no-one can see the information being typed if in a public space. Staff are encouraged to always choose the most secure connection—even if that means paying for access and then turning off the wireless network when it is not in use, or waiting until they get to the office or their home network.

Removable Media Policy

1. Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. USB sticks are the most common form of removable media, however optical discs, memory cards, and obsolete media such as floppy discs are also removable media. Most removable media is writeable, however some such as commercial CDs and DVDs is read-only.

Removable media is considered as such and must comply with these policies even if there is no intention to move it, for example an external drive that you always use on the same computer.

2. Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by EBCF and to reduce the risk of acquiring malware infections on computers operated by EBCF.

3. Scope

This policy covers all computers and servers operating in EBCF.

4. Policy

Removable media must be used only when necessary and data stored on it must be kept to a minimum. Data stored on removable media is at increased risk of loss or theft even if you comply with this policy. If you have files on removable media you **must** back them up elsewhere; the IT department cannot reasonably handle these backups.

Removable media may not be taken off EBCF premises without approval from a manager, who must confirm that there is a business need to do this and that the data cannot reasonably be transferred by another means, for example because it's too large or because it's a copyrighted disc.

Writeable removable media used with EBCF equipment must not be used with non-EBCF equipment or vice versa.

All removable media must have a single user and must be labelled, either physically or electronically or both, with that user's identity. Sharing of removable media between people is not permitted.

Removable media must be stored either on your person or in a locked drawer or cabinet.

All removable media used by EBCF staff must be encrypted with Bitlocker unless it qualifies for an exemptions below. Media that does not support Bitlocker and does not otherwise qualify for an exemption may not be used. The initial encryption process must be done on an EBCF computer, to ensure the recovery key is stored on EBCF's servers and nowhere else. Before using the device to store data you must request the IT department check that the recovery key was saved correctly.

Exemptions to encryption requirements:

- Read-only media that originates from outside EBCF, such as training DVDs.
- Media that must be written to by a device that does not support encryption, such as a camcorder. The data must be transferred to encrypted storage as soon as possible and deleted from the unencrypted media. EBCF computers, servers, and OneDrive are encrypted.
- Media that must be written to by a device that supports encryption other than Bitlocker, such as a Mac or Linux system. FIPS 140-2 compliant encryption must be used if available, otherwise an AES-256 solution, and if that is not available the data must be treated as though it was unencrypted.
- Media used to store PUBLIC data for distribution.
- Media to be handed over in person to a law enforcement officer, such as CCTV footage.

Exceptions to this policy may be requested on a case-by-case basis by EBCF-exception procedures.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Encryption
- Malware
- Removable Media
- Sensitive Information

Remote Working Policy

- **Objective**

When staff are required to work from remote locations, they shall ensure that sensitive data is not put at risk. The purpose of this policy is to inform staff about their own and the company's responsibilities regarding remote working and the use of mobile computer equipment or data storage devices outside company premises. Wherever staff are working, they must adhere to the same level of data protection as would be expected on company premises as set out in the company's "Information Classification Policy".

- **Scope**

The scope of the policy covers all individuals either employed or contracted to work with or for the company, either in-office or remotely.

- **Policy**

Regardless of the device used, it is the responsibility of the employee, contractor, vendor, agent, or third party to ensure that remote access is used in the same way as any local on-site connection to the company's network.

Teleworking refers to the act of dividing working hours between on-site and off-sitework. Remote working refers to any off-site working arrangement, be it teleworking or entirely remote working. This policy differs from the "BYOD Policy" in that it focuses on the use of company-owned and managed devices, rather than personal devices.

- Mobile computer equipment is defined as: any device that can store and process information electronically. This includes laptop computers as well as smaller handheld devices such as smart phones, USB devices and memory cards. [MP1] Chargers are also included and must be treated with the same care as the devices they go with. (Laptop chargers can be difficult and expensive to replace!)
- Company-owned mobile computer equipment must not be removed from company premises, or from storage areas within company premises, without authorisation from IT or a director.
- The company will keep a register of owned devices, and request that you sign any such devices in and out.
- Company-owned mobile computer equipment must be encrypted using industry standard methods before leaving company premises. The company's IT department will verify that this is the case before authorising a device to be signed out.
- When you have a device signed out, you are responsible for it. You must at all times keep it either in your immediate vicinity, or stored out of sight in a locked location such as your home or a hotel safe (but not a vehicle).
- Such equipment should never be left unattended in a staff member's car, on public transport or in the vicinity of anything related to commuting.
- Non-members of staff or unauthorised persons must not be given the use of company-owned computer equipment or storage devices.

- If using home computers, do so in line with the company's "BYOD Policy".
- Lock your screen when you are not using your computer or device. On Windows this can be done by typing ⊞+L or by clicking the person icon in the start menu. (Computers must be protected by passwords in line with the company's "Passwords & Authentication Policy").
- Staff making use of any device or equipment to access sensitive data must do so in accordance with the company's "Public Wi-Fi Policy".
- Any company-owned computer equipment must be used in line with the company's "Information Classification Policy". This includes rules such as not adding/removing/modifying software without authorisation and changing security controls.
- Home PCs and mobile devices must be regularly backed up in line with the company's "Backup Policy". Staff must make regular audits of what is stored on these devices.
- In the event that an employee leaves the company, any company-owned and managed devices in their possession will be remotely wiped immediately and must be handed back to the company at the next available opportunity.
- When discussing business in-person or on the phone, ensure that no sensitive information can be heard or seen by a third party.
- Paper documents containing sensitive data must be securely locked away when not in use. Any such documents that are disposed of must be destroyed in line with the company's "Disposal & Destruction Policy".
- Rules on the use of personally-owned devices for remote working or data storage are set out in the company's "BYOD Policy".
- Staff making use of any third-party equipment to access sensitive data must do so in accordance with the company's "Public Wi-Fi Policy".
- Staff must adhere to the company's "Information Classification Policy"..
- At all times, staff must take measures to secure sensitive data while working outside the business premises. This requires that staff:
- ensure sensitive information is not on view to people nearby (see the company's "Clear Desk Policy"). For example, this could include notes stuck to computer screens, minutes of meetings, financial reports and other items deemed sensitive by the company;
- when printing sensitive documents, always ensure that these are immediately collected from printers, fax machines or photocopiers;
- in no circumstances must personal computers be used for remote or home working without the relevant authorisation in line with the company's "BYOD Policy".
- The company may install location tracking software or hardware on its equipment. All tracking data will be processed in accordance with the GDPR, to protect the company's legitimate interest in preventing loss and theft of its assets, and will only be used for this purpose. If such tracking is installed, you will be informed of the details and given a GDPR statement when you sign the equipment out.

Change History Record

Version	Description of Change	Author	Date	Approved by
1.0	First version	Thomas	20/6/22	Suliman
1.1	Policy Review	Farhaan	12/06/23	Suliman
1.2	Policy Review	Farhaan	06/06/24	Suliman
1.3	Policy Review	Farhaan	17/01/25	Suliman
1.4	Policy Review	Farhaan	19/01/26	Suliman