CONSTRUCTION YOUTH TRUST

Information Security Policy

Reviewed and adopted by Board of Trustees: September 2023

Next Review Date Q3 2024

POLICY STATEMENT

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals personal data when it is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Construction Youth Trust (hereby referred to as 'the Trust') is dedicated to ensuring the protection of all information assets within the keeping of the Trust.
High standards of confidentiality, integrity and availability of information will be maintained at all times.

The Trust will demonstrate support for, and commitment to, information and cyber security through the issue and maintenance of an information security policy including the supporting guidance documents which are listed below.

This Policy sets out the measures taken by the Trust to achieve this, including to:

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support the Data Protection Policy in ensuring all staff are aware of and comply with UK law and our procedures applying to the processing of data; and
- increase awareness and understanding of the requirements of information security and the responsibility for staff to protect the confidentiality and integrity of the information that they process.

1. INTRODUCTION

1.1 Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

1.2 For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that stores data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

2. PURPOSE

2.1 Information is a major asset that the Trust has a responsibility and requirement to protect. The secure running of the Trust is dependent on information being held safely and securely.

2.2 Information used by the Trust exists in many forms and this policy includes the protection of information stored electronically, transmitted across networks and printed or written on paper. It also includes any information assets in Cyberspace (The Cloud). UK Cyber Security Strategy 2011 defined Cyberspace as:

“Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services”.

2.3 Protecting personal information is a legal requirement under Data Protection Law. We must ensure that we can provide appropriate assurances to our members and staff about the way that we look after information ensuring that privacy is protected, and personal information is handled professionally.

2.4 Protecting information assets is not simply limited to covering the information (electronic data or paper records) that we maintain, it also addresses who has access to that information, the processes they follow, and the physical computer equipment used to access them.

2.5 This policy details the basic requirements and responsibilities for the proper management of information assets.

3. SCOPE

3.1 This Information Security Policy and associated guidance documents, as listed below, apply to all systems, written, spoken and electronic information held, used or transmitted by or on behalf of the Trust, in whatever media. This includes information held on computer systems, paper records, hand-held devices and information transmitted orally.

3.2 This policy applies to all members of staff, including temporary workers, contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems. All members of staff are required to familiarise themselves with its content and comply with provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust’s Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

3.3 This policy does not form part of any individual’s terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

4. GENERAL PRINCIPLES

4.1 All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information). All data so classified must be handled appropriately in accordance with its classification.

4.2 All data stored on IT Systems or paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

4.3 All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the Data & IT Team or by such third party/parties as the Data & IT Manager may authorise. The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the Data & IT Manager unless expressly stated otherwise.

4.4 All staff have an obligation to report actual and potential data protection compliance failures to the Data Protection Officer who shall investigate the breach in line with our Security Incident and Data Breach Policy.

5. RISKS

5.1 The Trust recognises that there are risks associated with users accessing and handling information in order to conduct our business. We are committed to maintaining and improving information security and minimising its exposure to risks. It is our policy to use all reasonable, practical and cost-effective measures to ensure that:

- Information will be protected against unauthorised access and disclosure
- The confidentiality of information will be assured
- The integrity and quality of information will be maintained
- Authorised staff, when required, will have access to relevant systems and information
- Business continuity and disaster recovery plans for all critical activities will be produced, tested and maintained
- Access to information and information processing facilities by third parties will be strictly controlled with detailed responsibilities written into contract/documented agreements
- All breaches of information and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken.
- Information security training will be available to staff on request

5.2 Non-compliance with this policy could have a significant effect on the efficient operation of the Trust and may result in financial loss and embarrassment.

6. PHYSICAL SECURITY AND PROCEDURES

6.1 Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away, or destroyed as appropriate, to avoid unauthorised access.

6.2 Available locked filing cabinets and locked cupboards shall be used to store paper records when not in use.

6.3 Paper documents containing confidential personal information should not be left on office desks, on staffroom tables, or pinned to noticeboards where there is

general access unless there is legal reason to do so and/or relevant consents have been obtained.

6.4 The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Finance & Central Resources Manager as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

7. ROLES AND RESPONSIBILITIES

7.1 It is the responsibility of each member of staff to adhere to this policy, standards and procedures. It is the Trust's responsibility to ensure the security of their information, ICT assets and data. All members of the Trust have a role to play in information security.

7.2 The Data & IT Manager in conjunction with the IT Provider shall be responsible for the following:

- ensuring that all IT Systems are assessed and deemed suitable for compliance with the Trust's security requirements;
- ensuring that IT Security standards within the Trust are effectively implemented and regularly reviewed, working in consultation, and reporting the outcome of such reviews to the management;
- ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.

7.3 Furthermore, the Trust shall be responsible for the following:

- assisting all members of staff in understanding and complying with this policy;
- providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
- ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
- receiving and handling all reports relating to IT Security matters and taking appropriate action in response, including, in the event that any reports relating to personal data, informing the Data & IT Manager;
- taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
- monitoring all IT security within the Trust and taking all necessary action to implement this policy and any changes made to this policy in the future; and
- ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

8. All Staff

8.1 All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

8.2 Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

8.3 Staff must immediately inform the Data & IT Manager of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Security Incident and Data Breach Notification Policy.

8.4 Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the Data & IT Manager immediately.

8.5 You are not entitled to install any software of your own without the approval of the Data & IT Manager. Any software belonging to you must be approved by the Data & IT Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject. Prior to installation of any software onto the IT Systems, you must obtain written permission by the Data & IT Manager. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

8.6 Physical media (e.g. USB memory sticks or disks of any kind) may not be used for transferring files unless permission and device obtained from the Data & IT team. All devices must be returned to Data & IT team immediately after use to be wiped.

8.7 The Data & IT Managers approval must be obtained prior to transferring of files using a new cloud storage system.

8.8 If you detect any virus this must be reported immediately to the Data & IT Manager (this rule shall apply even where the anti-virus software automatically fixes the problem).

8.9 Work emails and accounts must only be accessed on or via work devices and not accessed or added to any personal accounts or devices

8.10 Work devices should not be used for personal use and should not have any software or applications installed for non-work purposes

9. ACCESS SECURITY

9.1 All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

9.2 The Trust has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the Trust’s network.

9.3 All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department.

9.4 All passwords must follow the Trust's password creation guidance (see Appendix 1)

9.5 Employees are required to store any passwords in KeePass, an encrypted password database. All KeePass details are linked to an employee's email and once an employee has left the trust, the database will be deactivated.

9.6 Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Data & IT. Any member of staff who discloses his or her credentials to another employee in the absence of express authorisation will be liable to disciplinary action under the Disciplinary Policy and Procedure.

9.7 Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

9.8 If you forget your password, you should notify the Data & IT Manager to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

9.9 Passwords should never be left on display for others to see. Computers and other electronical devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity.

9.10 All mobile devices provided by the Trust, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar.

9.11 Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this policy, the Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

9.12 All social media accounts will be password protected, and at least 2 members of staff will have access to each account and password including the Marketing and Communications Manager and Marketing and Communications Coordinator. Passwords for each account will be unique and secure (at least 8 characters in length containing numbers & symbols) and changed every 6 months.

10. DATA SECURITY

10.1 Personal data sent over the network will be encrypted or otherwise secured. All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Data & IT

Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the Trust's systems.

10.2 You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the Trust's Wi-Fi, provided that you follow the requirements and instructions governing this use. All usage of your own device(s) whilst connected to the network or any other part of the IT Systems is subject to all relevant Policies (including, but not limited to, this policy). The Data & IT Manager may at any time request the immediate disconnection of any such devices without notice.

11. ELECTRONIC STORAGE OF DATA

11.1 All portable data, and in particular personal data, should be stored on encrypted drives.

11.2 No data to be stored electronically on physical media e.g. USB sticks.

11.3 You should not store any business data on any personal device.

12. The handling, secure storage and retention of disclosure information

12.1 Reference from Gov.uk
https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information

As an organisation using the Disclosure and Barring Service (DBS) checking service to help assess the suitability of applicants for positions of trust, Construction Youth Trust complies fully with the code of practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information.

12.2 The Trust also complies fully with its obligations under the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of certificate information and has a written policy on these matters, which is available to those who wish to see it on request.

12.3 Storage and access
The Trust keeps certificate information stored securely in digital format with access strictly controlled and limited to those who are entitled to see it as part of their duties. Individuals retain the physical copy of their certificate.

12.4 Handling
In accordance with section 124 of the Police Act 1997, certificate information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom certificates or certificate information has been

revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

In addition, organisations that require retention of certificates in order to demonstrate 'safer recruitment' practice for the purpose of safeguarding audits may be legally entitled to retain the certificate. This practice will need to be compliant with the Data Protection Act, Human Rights Act, General Data Protection Regulation (GDPR), and incorporated within the individual organisation's policy on the correct handling and safekeeping of DBS certificate information.

12.5 Usage
Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Under no circumstances will the contents of a disclosure certificate be divulged to a person who is not authorised to have access to this information without the prior permission of the DBS applicant themselves.

13. COMMUNICATIONS, TRANSFER, INTERNET AND EMAIL USE

13.1 When using the IT Systems, you are subject to and must comply with the Acceptable User Policy.

13.2 Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee, and we cannot accept liability for the material accessed or its consequence.

13.3 All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email.

13.4 Postal and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

13.5 You should be careful about maintaining confidentiality when speaking in public places.

13.6 You should make sure to circulate confidential information only to those who need to know the information in the course of their work.

13.7 Personal or confidential information should not be removed from the Trust except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained.

13.8 You must ensure that the information is:

- not transported in see-through or other un-secured bags or cases;
- not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- not left unattended or in any place where it is at risk (e.g.in car boots, cafes, etc.)

14. REPORTING SECURITY BREACHES

14.1 All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Data & IT Manager. All members of staff have an obligation to report actual or potential data protection compliance failures.

14.2 When receiving a question or notification of a breach, the Data & IT Manager shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

14.3 Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Data & IT Manager. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Data & IT Manager.

14.4 Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Data & IT Manager.

14.5 All IT security breaches shall be fully documented.

14.6 Full details on how to notify of data breaches are set out in the Security Incident and Data Breach Notification Policy.

15. POLICY REVIEW

This Data Protection Officer is responsible for reviewing this policy. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

16. LINKS WITH OTHER POLICIES

This information security policy is linked to the:

- Data Protection Policy
- Security Incident and Data Breach Policy
- Record Retention Policy

The ICO also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of Information Law for use by organisations and the public. See www.ico.org.uk

Appendix 1

Password Generation

What makes a strong password?

The most important thing when considering generating new passwords is that the password has sufficient length and that the password is not used elsewhere. These precautions minimise the risk of brute force attacks or database breaches.

There are 2 recommended ways to generate passwords:

- Use Diceware (https://diceware.dmuth.org/) to create a list of at least 3 random words which can then be used as a password (we recommend also adding a number & symbol somewhere in the middle of the generated password). This makes the password much more 'human friendly' for the rare occasion that the colleague will need to type their password in as opposed to copying & pasting from their KeePass database.
- KeePass has its own included password generation feature which will generate a string of random characters, to generate a new password on KeePass:
    - Click the Add Entry button
    - In the Password field, a 20-character password with letters, numbers & capital letters will be automatically generated, use this password and add a symbol if required

Make sure to save your passwords in your KeePass database as per the KeePass guidance.