Data Security Policy

DATA SECURITY POLICY

Introduction

This policy sets out Evergreen's approach to managing the information required to conduct our business securely and confidentially.

It applies to all employees and other workers and to information held manually or electronically.

Where is our data held?

Some data is held in secure physical storage facilities on site.

Personal data is held confidentially on CARAS, with password controlled access.

Some data is held in Cloud-based file storage systems for data security and accessibility.

The Cloud-based systems we use are: Microsoft Office 365.

Additional storage options are provided for employees such as standard hard-drive memory on PC's.

Laptops and I-Pads are issued to Trustees, appropriate Office Staff, Chief Operations Officer and Chief Executive.

Data may also be held on our e mail exchange server – Microsoft Office 365.

Personal data on employees can only be accessed by Chief Operations Officer, Chief Executive and Office Manager.

Transfer of data

Employees may transfer personal data to authorised recipients using our e mail system.

Each e mail account is accessible only via unique user names and passwords distinct to individual employees.

Data held on e mail accounts is stored on dedicated server space in either the UK, EU or USA. Google are signatories to the EU-US Privacy Shield Agreement and have confirmed that they are compliant with all UK and EU regulations on data protection.

Personal devices

I-Phones are used for business purposes by staff with Evergreen. Any personal information will be sent password protected and must never be saved on a mobile phone. Where possible mobile phones must have a passcode on them. Should a mobile be phone stolen or lost it must be reported to the network provider so that they can block it and stop anyone from using it.

Virus protection

Everyone should abide by some simple rules to ensure the security and confidentiality of the Trust's IT network.

Employees must not install any software in the Trust's computers including laptops without prior authorisation from the Chief Operations Officer.

E mails or attachments from non-trusted sources should not be opened, as it is easy for viruses to enter the network. If you have any doubts about the source or content of an e mail, do not open it.

Password policy

Passwords protect the Trust's network and computer system. Care should be taken to keep passwords confidential. No one should attempt to gain unauthorised access to other computers or to confidential information they are not entitled to access.

Passwords must be unique to individual users, comprise a combination of letters and numbers, replaced regularly and if they were ever compromised.

In certain circumstances, such as sickness absence and holidays, employees may be required to share their passwords with their manager. However, it is not envisaged that passwords would be shared in other circumstances, other than between management.

If you leave your work station for any length of time, you should take appropriate action to protect confidentiality by logging off or activating your screensaver with an appropriate password.

Clear desk and clear screen policy

All information containing personal data should be put away in locked drawers or cupboards overnight or when away from your desk for an extended period of time.

Documents should not be saved to the desktop and computer screens should always be locked whenever you are away from your desk for an extended period of time.

Physical security

All data held by the Trust whether electronically or paper-based is protected by a number of physical security measures.

The building is accessed only via a lockable door and keys are issued only to designated key holders.

Outside of office hours the building is kept locked and secured by shutters and a key code alarm.

Electronic security

Data transferred in and out of the Trust is controlled and protected via a firewall system between us and our Internet Service Provider (ISP).

All our computers are further protected by a managed anti-virus and anti-malware system. IT support is available from 8am – 6pm and can be contactable out of office hours for advice.

Wireless internet access is provided within our office and secured by our ISP.

Acceptable use of computers and equipment

Computer facilities and other equipment provided by Evergreen are provided for business use only.

Equipment and facilities provided by Evergreen must not be used for personal reasons without permission having been granted in advance by the Chief Operations Officer.

Evergreen may monitor and intercept electronic communications (including e mail, voice and text messages) received at work in order to ensure the integrity of its IT systems or to prevent and detect criminal behaviour.

Please see our Data Protection policy for more information about the responsibilities and obligations that you and we both have in respect of personal data security.

It is also important that when using the Evergreen's computers and facilities you do so responsibly and in accordance with the rules set out in this Data Security policy and Use of Internet and E mail in our employee handbook.

Data breaches

Any suspected data breaches must be reported immediately to the Chief Operations Officer or to another senior manager, in line with Evergreen's Data Breach policy.

Serious or deliberate breaches of data security are listed in our disciplinary procedure as gross misconduct and may result in disciplinary action, including the termination of employment.

We believe that proper use of our computer systems will enhance the service that we provide to our customers and improve our efficiency and reputation.

Issue No: 1 June 2018

Date of Approval: 4th June 2018

Issue No: 2 September 2020
Issue No: 3 June 2021

Date of Approval: 2nd June 2021