TalentEd

Expert teachers for bright students

Information, Technology and The Collection of Data Policy

Issue 1 May 2018

Contents

Introduction

This policy sets out the Charity's guidelines regarding acceptable use of the computer systems and networks by all employees alongside the Charities policy on the collection, storage and use of data.

As these services and systems provide such a vital and integral part of the Charity's infrastructure and this policy meets a legislative requirement it should be clear that this policy must be strictly adhered to and that any breaches may give rise to disciplinary action.

If the offence is serious, it may well constitute gross misconduct, particularly if it involves indecent material, sexual or racial harassment, the unauthorised sharing of sensitive or personal data or illegal activities.

Confidentiality

All data created and stored on the Charity network is the property of the Charity, and the Charity holds all copyright in such data. This holds true for all data, whether or not it was created for personal or business use.

The Charity complies with all aspects of the Data Protection Act and General Data Protection Regulations. Any data collected must not be retained for any period or purpose other than that for which its use has been authorised and must be disposed in an approved manner and as agreed with the Data Controller once that approval is removed or expires.

Whilst every effort is made to ensure confidentiality and security of data it is not possible to guarantee this. Should you have any extremely sensitive data you should contact the charity's Data Controller to have the access restricted to your specific requirements. These permissions can be applied to individual files or folders containing multiple files.

Passwords

You are responsible for the security of data, accounts and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

Passwords should be "complex" and consist of at least 8 characters. They should be made up of a combination of upper case and lower case letters, punctuation marks and numbers. Network users are prompted to change their password every 42 days.

Virus Protection

Anti-virus software is loaded on all computers as standard and is updated regularly over the network. Anti-virus software must not be de-installed or deactivated. If you are in any doubt of the status of your virus protection you must immediately contact the Data Controller. Remote users are responsible for maintaining up to date virus definitions on their computers and can contact the Data Controller for help as required.

Extreme care should be taken when opening all attachments to emails, even those that appear to have been sent from trusted sources.

If there is any doubt as to the trustworthiness of any files. **Do not open or download the file**, the Data Controller should be contacted to discuss testing for viruses.

Unauthorised software and hardware

All PCs within the Charity have the necessary software and hardware installed on them. No other software or hardware may be installed without the express permission of the Data

Controller. All software used will be purchased, registered and licensed in the charity name and used as permitted by the licensing agreement.

TalentEd does not permit users to install or use unauthorised software or copy or remove software.

No personal hardware includes items such as laptops, PCs, laptops, hand held androids, USB Pen Drives, smart phones should be attached to the network without authority from the Data Controller.

To maintain security and serviceability, all hardware and software is to be sourced through the Data Controller in accordance with Charity Policy.

Removable media, (Pen Drives, floppy disks, etc)

Removable media can be defined as any portable device that can be used to store and move information. Media devices can come in various formats, including but not limited to:

- USB memory sticks (also known as flash disks or drives)
- Compact disks (CD)
- Digital Versatile Disks (DVD)
- USB Hard Disk Drives
- MP3 /MP4 players (such as IPods or any other brands)
- Mobile Phones and other androids
- Digital Cameras

These devices create the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorized people, outside the Charity, potential access to Charity passwords and other confidential information.

The use of such personal media is restricted; however should you require access to Charity Removable Media please request this via the Data Controller.

Email

Use of email by employees of TalentEd is permitted and encouraged where such use supports the goals and objectives of the business.

However, the employee must ensure that they:

- Comply with current legislation
- Use email in an acceptable way
- Do not create unnecessary risk to the charity.

In particular the following is deemed unacceptable use or behaviour by employees:

- Forwarding of charity confidential messages and data to external locations
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- Accessing copyrighted information in a way that violates the copyright.

- Chain letters or mass mailings.
- Breaking into the charity's or another organisation's system or unauthorised use of a password/mailbox
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- Transmitting unsolicited commercial or advertising material
- Undertaking deliberate activities that waste staff effort or networked resources
- Introducing any form of computer virus or malware into the corporate network

TalentEd accept that the use of email is a valuable business tool; however, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.

Internet Access

Use of the internet by employees is permitted and encouraged where such use supports the goals and objectives of the business.

However, the employee must ensure that they:

- Comply with current legislation
- Use email in an acceptable way
- Do not create unnecessary risk to the charity.

In particular the following is deemed unacceptable use or behaviour by employees:

- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Using the internet to send offensive or harassing material to other users
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- Hacking into unauthorised areas
- Publishing defamatory and/or knowingly false material about TalentEd, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format
- Revealing confidential information about TalentEd in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions
- Undertaking deliberate activities that waste staff effort or networked resources
- Downloading, storing or sharing data without the appropriate approvals and/or in a way that might conflict with other policies e.g. Safeguarding
- Introducing any form of malicious software into the corporate network

If you produce, collect and/or process business-related information during your work, the information is covered by the Data Protection Regulations and must be secured securely and not shared without approval from the Data Controller. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

TalentEd accept that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business. In addition, all of the charity's internet-related resources are provided for business purposes. Therefore, the charity maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited.

Monitoring

At any time and without notice, we maintain the right and ability to examine any systems and inspect and review any and all data recorded in those systems. Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by the TalentEd. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists the management of information systems.

In order to ensure compliance with this policy, TalentEd may employ monitoring software to check on the use of the internet and block access to specific websites to ensure that there are no serious breaches of the policy. We specifically reserve the right for authorised personnel to access, retrieve, read and delete any information that is created by, received or sent as a result of using the internet, to assure compliance with all our policies. Such monitoring will be used for legitimate purposes only.

Breaches of this Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

Authorised by: ……………………………………………….

Date: ……………………………………………………..