The IT Code of Practice

Introduction

Your guide to using IT at Barnardo's

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of everybody accessing Barnardo's systems to read and know this code of practice, and to conduct their activities accordingly. Barnardo's IT code of practice must be followed by all users of Barnardo's IT systems. No unauthorised use is permitted.

Purpose:

- To support the confidentiality, integrity and availability of information in Barnardo's.
- To ensure computing resources, information and information processes are consistently protected according to approved organizational security practices, legal and regulatory requirements.
- To clearly define acceptable usage of Barnardo's IT Systems.
- To clearly define acceptable usage of any social network or blog by staff or volunteers, during or outside of working hours.

Scope:

- This code of practice applies to all information stored electronically within Barnardo's and to all use of Barnardo's computing resources.
- This code of practice applies to all IT Users: employees, contractors, volunteers, secondees and all other third parties who have authorised access to Barnardo's premises and computing resources.
- Barnardo's monitors for compliance with the code of practice. Appropriate investigation may take place where breaches of this code are suspected. This may include quarantine of IT equipment, viewing of emails, Internet and other computer records or information. Breaches of the code may result in disciplinary action being taken, up to and including dismissal and legal proceedings.
- Aiding or coercing breaches of this code of practice will be deemed as equal responsibility for the action of the perpetrator.
- This code of practice applies to all use of social networks or blogs by staff or volunteers, during or outside of working hours.

Confidentiality

Both during and after your work-life at Barnardo's, certain information related to Barnardo's business must be treated confidentially and must not be used or disclosed unless authorised. This includes all personal information, confidential and sensitive material relating to the management and operation of Barnardo's, eg, bids and tenders, staff salaries, staff appraisals, certain financial information etc. You should not disclose any documentation or information in any form (including copies or in written or any other format) created for Barnardo's use.

Data Security

Barnardo's has legal and regulatory responsibilities that determine how we process data. We must carefully control where data is stored, who has access to it and prevent unauthorised disclosure. Barnardo's IT resources - data, information and information processes - must be protected. You should ensure that:

- You only access data, equipment, software or information that you are authorised to access.
- You do not cause malicious damage of any sort.
- You always lock any device you are using, before leaving it unattended.
- You pay close attention to the physical security of devices in public places.
- You turn off your PC before leaving the premises, unless there is a valid reason to leave it on.

Confidential data should only reside and be accessed from Barnardo's corporate IT systems (eg Content Server and SharePoint) or from authorized third-party systems (eg, external service user recording systems, external payroll systems, external pension systems) or from your personal device via Azure Virtual Desktop.

- Authorisation for processing confidential data on third party systems is given by the Head of Operating Technology and can be verified by reference to the IT Service Desk.
- Confidential data should only be transferred using approved systems such as OneDrive or SharePoint
- Files containing confidential data should be kept on the agreed storage system. However, working copies may be stored locally, where there is a business need. Any updated file must be uploaded to the appropriate storage system at the first opportunity.

It is the responsibility of every line manager to ensure that the staff and volunteers that report to them have the appropriate level of access to business systems, which is managed through the Starters and Change Management Processes.

All security incidents or concerns should be promptly reported to the IT Service Desk on 0330 222 0199.

Data Protection

Barnardo's must comply with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act of 2018 (DPA18).

These regulations apply to any information which relates to identifiable, living individuals and to whatever medium is used to record the data, e.g., paper, computer or CCTV. Your responsibilities to ensure the confidentiality, integrity, and availability of personally identifiable information can be found in Barnardo's Data Protection Policy.

Other Information Security Policies

Other Information Security Policies, that complement the IT code of practice, can be viewed in the relevant policy section on Inside Barnardo's.

Your acceptance of Barnardo's IT Code of Practice
All users of Barnardo's IT Systems are required to agree to the terms of the IT code of practice each time they log in.

Breaches of Barnardo's IT Code of Practice
We would consider each breach of the IT code of practice carefully and individually. We would prefer to resolve any issue arising out of such a breach informally. However, if the matter is sufficiently serious it may result in disciplinary action including dismissal. If the breach constitutes a posting on a social media network which breaches this IT code, Barnardo's will also ask you to remove the content.

Passwords and Logins
A login with a password is a unique key for accessing Barnardo's IT Systems. Ensure you:

- Choose strong passwords (at least 10 characters with a mix of uppercase and lower-case letters, numbers and other symbols) that others cannot easily guess or work out. It cannot contain parts of your username and it cannot be the same as a password previously used in the last 24 months.
- Never reveal your password to anyone or allow others to use your login and password

Further information on resetting your password can be found here:
Resetting your passwords and changing your details | Inside Barnardos

Access to Barnardo's systems
Barnardo's recognizes there may be instances when you use your own (non-Barnardo's) IT device. You must use Azure Virtual Desktop and our multifactor authentication tool, OKTA so you can work securely. Guidance on how to do this can be found on Inside Barnardo's:
Setting up a personal device for Barnardo's systems | Inside Barnardos
Microsoft Azure Virtual Desktop (AVD) | Inside Barnardos
Setting up a Barnardo's laptop, desktop, tablet or smartphone | Inside Barnardos

Access from non-Barnardo's Premises
Take care when accessing Barnardo's confidential data. Think when working outside Barnardo's premises, e.g., using a Barnardo's laptop in a public place, who might possibly be able to see any data on the screen. The more sensitive the data, the more precautions around data security should be observed. Please see the Homeworking Policy on Inside Barnardo's for further information.

Email, internet, social media and virus and spyware prevention

Email
Barnardo's provides email for legitimate business communication. Barnardo's owns the copyright of email and can retrieve and view email (even after IT users delete messages from their email accounts). All business emails must be sent from a Barnardo's email account. You are

responsible for what is sent from your email account. Care must be taken over the content of any message and must not:

- Include offensive content (including images, videos or other media), in respect to pornography, race, gender, sexual orientation, disability, age, gender reassignment, religion/belief or politics.
- Include any swearing or other unacceptable use of language.
- Constitute harassment or bullying of any sort.

To protect Barnardo's from business and associated reputational risk, external emails are monitored for offensive content. Remember external email goes out bearing Barnardo's email footer – the equivalent of sending a letter with a business letterhead. When using the Barnardo's email system:

- As a safeguard against fraud, you should never provide your personal data via email or in response to an email.
- It's strongly recommended that sensitive or confidential data should be sent encrypted if sent external to Barnardo's. Remember information is not secure when sent externally unless it is encrypted.
- Take care over wording of messages as it is possible to set up a legally binding agreement by email.
- Messages may be opened in your absence, but only in exceptional circumstances.
- It's not generally permitted to send emails to all (or large groups of) IT users. Only certain employees are authorised to do this.
- Do not open attachments or click on links if you are at all suspicious of an email message. You are not permitted to distribute chain mail.

Occasional personal emails may be sent (and received) from your Barnardo's email account where they satisfy the criteria laid out in this section.

Use of internet

The Internet, including social media sites, is a critical business resource, allowing employees to carry out legitimate business activity more effectively. However, as an information resource it presents a business risk and needs to be used within clear guidelines. When using the internet, you should ensure that you:

- Do not access Internet sites which contain offensive material of any sort. That is, offensive in respect to pornography, race, gender, sexual orientation, disability, age, gender reassignment, religion/belief or politics.
- Do not download or store any offensive material (especially pornography).
- Do not access or place any material on the Internet that might be considered inappropriate, offensive or disrespectful to others.
- Only use approved file transfer services, such as OneDrive or SharePoint or a tool approved by a commissioner, for the transfer of confidential information.
- Do not use the Internet for personal gain or profit.

Barnardo's provides access to the Internet as a business tool. You are responsible for all Internet sites accessed under your login. The browsing histories of staff using Barnardo's devices can be accessed when appropriate

Social media
Use of blogs or social networks, such as Facebook or Twitter, has become ubiquitous and central to much business and social life. Whilst our starting point is that what people say or do outside work on these networks is private, Barnardo's also recognises that its reputation and people are key assets and everyone working here shares the responsibility of protecting them. If on a social media network, you refer to Barnardo's, its work or your colleagues, or could be identified as being associated with Barnardo's, you should ensure that your postings do not damage the reputation of Barnardo's or its employees.

This includes direct or indirect criticism or stating a position that is averse to the interests of Barnardo's.

- Respect your colleagues and never publish comments which could amount to harassment or bullying.
- Do not disclose any confidential information which relates to the business of Barnardo's.
- Do not misuse any personal data relating to your colleagues. You can also refer to the Social Media Policy for more information.

Virus and Malware prevention
Computer viruses, spyware and malware can disrupt and damage Barnardo's IT systems and business. This means:

- Viruses and malware must be prevented from gaining access to Barnardo's IT Systems. Do not maliciously allow viruses, spyware or malware onto Barnardo's IT Systems.
- Software, documents, discs and external recording materials (e.g., USB memory sticks) may carry viruses or spyware. Internet downloads can also introduce viruses and spyware onto IT systems. Take care of what is accessed on Barnardo's IT Systems - using trusted sources minimises risk to Barnardo's.
- Do not tamper with the anti-virus, anti-spyware or any other security software installed on a Barnardo's device.

Software, procurement, donated equipment and disposal

Software
It is the legal obligation of Barnardo's and its employees to comply with copyright laws and respect the intellectual property rights of others. You are not permitted to:

- download or use unlicensed software or computer files (including unlicensed mp3 files and other music or media files) on Barnardo devices.
- Possess, use, reproduce or distribute software on any Barnardo's device without authorisation.
- No unlicensed files (including mp3 files and other music or media files) are permitted to be used or stored on Barnardo's Systems. Only software approved by Operational Technology is permitted to be loaded onto a Barnardo's machine or downloaded from the Internet. Software and software licenses may only be purchased or obtained through the procurement process.

Procurement
All Barnardo's IT hardware equipment, software and telecommunication lines must be procured through the Operating Technology department. This includes educational and specialist

hardware and software. Exceptions are very rare and require prior approval from a senior manager in Operating Technology.

If you are procuring any non-standard hardware or software, please seek technical advice from Operating Technology. For instance, if what you're procuring runs through Barnardo's technical platforms and operates on our network, eg, an electronic visitor's book, you will need to ensure that it will work within the parameters of the firewalls set up to protect us. It's important to do this in advance.

You can go to My IT Store in FirstPoint to order new equipment and software.

Donated equipment
Any donated equipment received will be classed as a personal device which is the responsibility of the owner of the device to maintain. These devices will not be supported by Operating Technology.

Disposal of computer equipment and media
When Barnardo devices are no longer required or are to be replaced, they must be decommissioned securely. Under no circumstances should computer equipment be given away, dumped or passed to a new section of Barnardo's, as data can be obtained from disks not decommissioned by Operating Technology. If this procedure is not followed, information sensitive to Barnardo's could become available to unauthorised individuals and cause a breach of the UK GDPR.

All computer equipment disposals must comply with the Waste Electrical and Electronic Equipment (WEEE) Directive: all Barnardo devices that are able to access Barnardo's systems, or that contain business sensitive or personal data should be returned to Operating Technology for secure disposal; all other equipment is the responsibility of local management. See the equipment returns process

Responsibilities for Equipment
All equipment must be treated with respect, care and kept clean, if you have equipment assigned to you personally, i.e laptops or phones, you are responsible for them and the usage of the device.

When you leave Barnardo's, your IT equipment must be returned to the IT Supply Department at Barnardo's House immediately following our returns procedure.
Please inform your line manager of the consignment number provided in case there are any issues or queries.

The Operating Technology team must be advised if you intend to give your equipment to someone else. You must also advise Operating Technology if you change office location, move to home working or change name.

If any equipment becomes faulty, an IT ticket must be made to the IT Service Desk, giving full details of the problems being experienced. Please do not raise a request for new equipment.

Under no circumstances can SIM cards be swapped between mobile handsets or tablets. Equipment must not be removed from offices; The IT Supply Team must be contacted in the first instance before the equipment is removed.

All equipment that is no longer being used must be returned immediately. Please keep all courier documents in case of any queries or issues.

Getting Help with IT

Please refer to the guidance below if you need to seek support from the IT ServiceDesk, including reporting faults and ordering new equipment, etc.
Getting help with IT | Inside Barnardos

Date	Version	Review Period	Changes	Author	Authorised
June 2023	2	2 Years (unless significant changes to systems or process)	Updated to reflect move from On-Prem to Cloud, Homeworking and changes to IT Security Management	Martine King	Kieron Thorpe Martine King