FCA DATA PROTECTION SECURITY POLICY

INTRODUCTION

The Data Protection Act 2018 covers all Personal Data (PD), whether on paper or in electronic format. It enacted the EU General Data Protection Regulation (GDPR) into UK Law. There is also a UK-GDPR which takes over from the EU GDPR on 31 Dec 2020. There are certain differences, but little for us.

This document should be read in conjunction with FCA Data Protection Policy covers the overall FCA data protection policy.

PD includes any personal opinions relating to individuals expressed by FCA volunteers in an FCA environment. The Act also defines 'sensitive information', such as racial or ethnic origin and religious or other beliefs. FCA policy is never to hold Sensitive Data on any individuals.

GDPR requires all personal data to be handled in a manner that ensures its appropriate security:

1. All PD must be held securely whether in paper form (locked away) or on computer / tablet / phone (password protected and preferably encrypted).
2. FCA policy is not to hold any 'Sensitive data', which is defined as PD relating to political leanings, sexual orientation, race, medical information, etc. This is subject to additional security requirements. Tell the Treasurer ASAP if you need to store sensitive data.
3. ICO compliance requirements state that FCA must have measures in place to keep the personal data FCA holds safe and secure.
4. FCA must have measures and procedures in place to detect, investigate, and report data breaches. Data breaches must be handled in accordance with the FCA "Action in the event of a data breach" instructions, and reported to the ICO when appropriate.

PHYSICAL SECURITY OF PERSONAL DATA

5. Hard Copy. When not in use, all hard copy (paper) PD is to be locked away in a cabinet or drawer.
6. Digital Devices. When not in use, all digital devices containing FCA PD (desktop, laptop, tablet, phone, and storage devices such as memory stick or external hard drive) are to be kept physically secure, ie, desktop computers should be shut down, and all portable devices memory storage are to be locked away.

CYBER SECURITY OF PERSONAL DATA

7. Risk Management Regime. Key risks are:
    a. Phishing Attacks - to pretend to be a trusted contact to entice a user to click on malicious links or downloads to gain access to sensitive data, account details or credentials.
    b. Malware Attacks – to insert malicious code or software to gain access to networks, or steal data or destroy data. It usually comes from malicious downloads, spam emails or connecting to infected computers.
    c. Ransomware Attacks – involving encrypting data so that it cannot be used by FCA, and demanding a ransom to release the data.
    d. Lack of Threat Awareness – if users do not understand the types of threat they may face and the damage they can do, they are more likely to inadvertently enable malicious access to FCA accounts.

e. Weak Passwords – the use of weak or easily-guessed or using one password on many accounts simplifies malicious access to accounts to steal data etc.

f. Other Risks Include:

i. Compromise of email accounts through downloading malware or lack of 2-factor authentication.

ii. Compromise of PD in files held on computer or online.

iii. Compromise of email address PD by not using bcc in emails.

iv. Loss of PD through computer hard drive failure or inadvertent deletion.

8. Network Security.

a. To protect your network from attack, volunteers are to ensure that their router is password-protected with an effective password, with recommended security settings.

b. Volunteers are to avoid wherever possible connecting to an untrusted or insecure network. If essential, they are to have a working Virtual Private Network (VPN) in place before connecting a device containing FCA PD to an untrusted or insecure network.

9. Malware Prevention. Volunteers are to ensure that they have effective anti-virus solutions that actively scan for malware in both incoming and outgoing communications.

10. Removable Media Controls. The use of removable media such as memory sticks and external hard drives is to be kept to a minimum. Where it is essential, it is to be limited to word processing, spreadsheet and presentation material. No executable files are to be loaded onto them. Any removable media must be scanned by antivirus prior to the importing any data onto a device holding FCA PD, and must be kept locked away when not in use.

11. Secure Configuration. Volunteers are to keep any device containing FCA PD up to date with the latest operating system software. This will minimise the risk of software weaknesses exposing the device to threats and vulnerabilities.

12. Home and mobile working. All volunteers will be using their own devices for FCA work and holding FCA PD. The cyber security section of this policy is written with this in mind. Additional points are:

a. Volunteers should keep the number of devices holding FCA PD to one, unless absolutely essential, in which case approval to do so should be sought from the Treasurer using a VPN.

b. Devices should be encrypted if the device supports it and protected away from home through the use of a functioning VPN.

13. User Education.

a. The FCA Data Protection Guidance document is provided to cover all aspects of data protection, but includes a section on cyber security.

b. Awareness is maintained through regular reminders of good practice, and annual security reviews.

c. Consider specialist training for Treasurer.

14. Incident Management – under GDPR, FCA must report a serious data breach to the Information Commissioner's Office within 72 hours. Top Level Plan is as follows (Cyber Security Response and Recovery guide). See detailed plan for more information:

a. Step 1. Prepare for incidents.

b. Step 2. Identify what is or has happened.

c. Step 3. Resolve the incident.

d. Step 4. Report the incident to the wider stakeholders.

e. Step 5. Learn from the incident.

15. Monitoring – is to be carried out by users on a continuous basis with a review each month of key aspects of security as follows:

    a. By volunteers on their own devices.

    b. By the Treasurer on the FCA Microsoft 365 system and files held in the FCA Sharepoint account.

16. Managing user privileges – access to different aspects of FCA work is to be limited to those who need the access to complete their work. Access, especially to Sharepoint files, is to be reviewed annually, or when there is a change of personnel in a post.

GOOD PRACTICE.

17. Password-protect your devices to prevent unauthorised access to your files (this also encrypts iPads and iPhones).

18. Use effective passwords – different ones for each account. Use either:

    a. Three random words (five letters minimum) with no spaces in between, or

    b. A minimum of eight (preferably more) random characters including at least one of each of the following: capital and lower-case letters, numbers and special characters such as & or *, or

    c. A combination of i and ii above.

19. Use two-stage authentication wherever possible to make logging in or changing passwords much more secure.

20. Keep your operating systems, software programs and apps up to date.

21. Encrypt your devices where possible.

22. Encrypt/password protect all computer PD files and folders.

23. Ensure you have a firewall and an up-to-date anti-virus program on any device holding FCA PD.

24. Run regular anti-virus scans on your device.

25. Where possible, store computer files online.

26. Check your email and other settings frequently to ensure that they have not been tampered.

    a. In particular, check email settings to ensure that there no unauthorised forwarding rules have been inserted or other unauthorised changes to settings.

    b. Also for online cloud storage, check there are no unauthorised sharing rules inserted.

27. When sending FCA emails, ensure that the appropriate data protection wording and link to the Privacy Notice is added at the bottom.

28. Be suspicious of any odd or unusual emails, texts or phone calls even if purporting to come from a known source. Do not click on any links in texts or emails unless you are certain they are safe.

29. For security and privacy reasons, when writing emails, use the blind copy option (BCC) address slot instead of To or CC slots for email addresses when emailing more than two people or where addressees may not know each other's email. Put your own email address in the To line. This keeps individuals' email addresses secure and protects their privacy by not revealing their email address to those who might not already know it.

WHAT TO AVOID:

32. Holding any sensitive personal data, eg, racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexual life, criminal proceedings or convictions.
33. Holding personal data without a lawful basis for doing so.
34. Leaving personal data unattended or insecure, eg on a desk, in an unlocked file or unprotected on a computer.
35. Giving out personal data to third parties without the data subject's written consent
36. Giving out personal data over the telephone without a lawful basis for doing so.
37. Making public any personal data or photographs of individuals without their written consent, eg, on a noticeboard, in publicity material, or on the Web
38. Destroying or altering PD following the receipt of a Subject Access Request before providing a copy of the PD to the individual.
39. Sending personal data abroad.

FCA GDPR DOCUMENTATION

40. Action in the event of a data breach.
41. Action in the event of a Subject Access Request.
42. Action in the event of any other Subject Request.

Updated 14 Dec 2020