The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

To: Finham Park Multi Academy Trust

Of: Green Lane, Finham, Coventry, CV3 6EA

The Information Commissioner (the Commissioner) issues a reprimand to Finham Park Multi Academy Trust ('Finham Park') in accordance with Article 58(2)(b) of the UK General Data Protection Regulation in respect of certain alleged infringements of the UK GDPR.

The reprimand

The Commissioner has decided to issue a reprimand to Finham Park in respect of the following alleged infringements of the UK GDPR:

- Article 5(1)(f) which states:

  "*personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*".

- Article 32(1) which states:

  "*taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*."

The reasons for the Commissioner's findings are set out below.

Article 5(1)(f) and Article 32(1)(b)
Technical and Organisational Measures – Access Controls

- Finham Park did not have appropriate technical measures in place to ensure the confidentiality and integrity of their systems. Finham Park had an inadequate account lockout policy, and reversible password encryption was enabled[1]. The National Cyber Security Centre ('NCSC') recommends having appropriate account lockout[2] in place. Had these elements been addressed sooner, it could have significantly reduced the likelihood of a successful attack.

- Finham Park did not have multi-factor authentication ('MFA') in place. Extensive guidance was available via the NCSC which promotes the use of multi-factor authentication.[3] Additional means of authentication serve to make unauthorised access more difficult and help to protect particularly sensitive personal data.

- Finham Park did not ensure that its employees had sufficient knowledge and understanding around the re-use of passwords. The NCSC emphasises that passwords should not be re-used across accounts[4]. Had Finham Park educated its employees on password management more effectively, it is possible that this incident could have been avoided.

Aggravating factors

Finham Park reported three similar incidents to the Commissioner and each time the Commissioner provided guidance to Finham Park, which set out the importance of implementing appropriate password policies and account management procedures. Finham Park failed to follow this guidance and failed to implement appropriate technical and organisational measures to secure its systems. The Commissioner's Regulatory Action Policy sets out that where the Commissioner has issued advice, and this advice is not followed, the Commissioner will take this into account as an aggravating factor.

---

[1] Modify Authentication Process: Reversible Encryption, Sub-technique T1556.005 - Enterprise | MITRE ATT&CK®
[2] Password policy: updating your approach - NCSC.GOV.UK
[3] Multi-factor authentication for online services - NCSC.GOV.UK
[4] Living with password re-use - NCSC.GOV.UK

Remedial steps taken by Finham Park

The Commissioner has also considered and welcomes the remedial steps taken by Finham Park in light of this incident. In particular, Finham Park restored its systems from backups, implemented MFA across the trust, and signed off a digital transformation project plan, which included credential monitoring.

Decision to issue a reprimand

Taking into account all the circumstances of this case, including the aggravating factors and remedial steps, the Commissioner has decided to issue a reprimand to Finham Park in relation to the alleged infringements of Article 5(1)(f) and Article 32(1) of the UK GDPR set out above.