Ministry
of Defence Police

Data Protection Officer & Freedom of Information Manager

Room 126 Building 1070

MDP Wethersfield

Braintree CM7 4AZ

United Kingdom

Telephone: +44 (0)1371 85[redacted]

E-mail: MDP-FOI-DP@mod.gov.uk

[redacted]

[redacted]

Our Ref: eCase: FOI2018/07931 RFI:186/18

Date: 5 July 2018

Dear [redacted]

FREEDOM OF INFORMATION ACT 2000. MINISTRY OF DEFENCE POLICE: INFORMATION TECHNOLOGY

I refer to your e-mail of 5 June 2018, which was acknowledged on 14 June 2018. We are treating your e-mail as a request for information in accordance with the Freedom of Information Act 2000 (FOIA 2000).

In your e-mail you requested the following information:

Annex A – attached.

A search for information has now been completed by the Ministry of Defence Police and I can confirm that we do hold some information in scope of your request – see Annex A.

If you have any queries regarding the content of this letter and the Annex, please contact this office in the first instance.

If you wish to complain about the handling of your request, or the content of this response, you can request an independent internal review by contacting the Information Rights Compliance team, Ground Floor, MOD Main Building, Whitehall, SW1A 2HB (e-mail CIO-FOI-IR@mod.gov.uk). Please note that any request for an internal review should be made within 40 working days of the date of this response.

If you remain dissatisfied following an internal review, you may raise your complaint directly to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not normally investigate your case until the MOD internal review process has been completed. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website at https://ico.org.uk/.

Yours sincerely

MDP Sec Data Protection and Freedom of Information Office

Question	Answer
1) Does your force currently follow the basic password practices set by the NCSC?	■ YES ☐ NO (if not followed please specify here where guidance is sought from)
2) What steps has your IT department taken to assist to simplify password policy for front line officers? And support staff?	Allow users to choose user generated password that follows complexity requirements.
3) How often do systems require the end-user to renew their password?	☐ Less than 60 days ☐ 61 -90 days ■ 90 days or more ☐ No requirement in place
4) What training is given to staff and front line officers with regards to best practice when using passwords? (eg avoid using simple passwords such as Passwrd123, or even recycling passwords?)	Guidance available from IT Service Desk, Quick Reference Guides and on-line virtual agent.
5) If no training is provided has consideration been given to training to be delivered? If not training what options have been taken(eg regular emails, etc)?	N/A
6) Factory-set default passwords being left unchanged is one of the most common password mistakes that organisations make. Does your force immediately change factory set defaults prior to asset deployment?	■ YES ☐ NO
7) What does your force do to help users cope with 'password overload'?	Provide advice, guidance and policy via IT Service Desk, Quick Reference Guides and on-line virtual agent.
8) Is there a password management system in place? Or are there other solutions offered?	☐ YES ■ NO
9) Is there any password monitoring in place?	■ YES ☐ NO
10) Do staff with administrator accounts have separate "standard" user accounts?	■ YES ☐ NO
11) Do remote users (Mobile and laptop) use VPNs?	■ YES ☐ NO

12) Does your force use an account systems lockout and protective monitoring system?	■ YES ☐ NO
13) Does your force have a password blacklisting policy/system? (password blacklisting will disallow the most common password choices).	☐ YES ■ NO
14) Is your force IT department regularly communicating password practices for staff to follow?	■ YES How often ? Continuous via IT Service Desk, Online Virtual Agent and published Quick Reference Guides. ☐ NO
15) Is there a password policy and may I have a copy?	■ YES ☐ NO This document is owned by MOD Information Systems and Services (ISS). An approach to them will need to be made to release this document.
16) Is two-factor authentication used in the force?	☐ YES ■ NO Please specify if and which alternative methods of sign in are used?
17) Are there any systems which have automatic sign in option by the means of one click? Eg crime recording software?	■ YES ☐ NO
18) Has your force carried out any surveys internally to asses if staff are following good password hygiene practices? (eg recycling them?)	☐ YES ☐ NO Not Known – Such surveys are the responsibility of MOD Information Systems and Service (ISS)
Please insert any further comments or information you feel may be relevant	