

PFCC Decision Report

Report reference number: 052/2020

Classification: Not protectively marked

Title of report: Use of Communications Policy

Area of county / stakeholders affected:

The PFCC, all permanent, temporary and agency staff, contractors and volunteers.

Report by: Pippa Brent-Isherwood (Chief Executive and Monitoring Officer)

Date of report: 14 April 2020

Enquiries to: Darren Horsman (Strategic Head of Policy and Public Engagement)

1. Purpose of the report

To approve the updated Use of Communications Policy.

2. Recommendations

That the updated Use of Communication Policy attached at Appendix 1 is approved for adoption.

3. Benefits of the proposal

A clear and up to date Use of Communications Policy is an essential tool in ensuring that the Police, Fire and Crime Commissioner (PFCC), and all their permanent, temporary and agency staff, contractors and volunteers, uphold the standards expected of those representing the PFCC and their office. The updated policy attached for approval at Appendix 1 describes the specific user standards relating to the following:

- Internet access and usage;
- Email usage;
- Telephone systems including mobile telephones, and
- Remote working and mobile computing devices.

4. Background and proposal

The Use of Communications Policy has been reviewed and updated as part of the PFCC's ongoing policy review plan. In particular, a new section has been added relating to remote working and mobile computing devices.

The policy will be reviewed again in three years' time, or sooner if required by changes in legislation, regulations or best practice.

5. Alternative options considered and rejected

The PFCC could chose not to adopt the updated Use of Communications Policy, and therefore effectively to "hold over" on the existing policy. This course of action is not recommended as to do so would provide staff, contractors and volunteers with insufficiently clear guidance as to the standards expected of them, particularly in relation to remote working and mobile computing devices, which play an increasingly important part in the job roles of PFCC staff.

6. Police and Crime Plan

Effective use of technology – including information and communications technology – is one of the underlying principles of the Police and Crime Plan.

7. Police operational implications

The policy has been reviewed alongside comparable Essex Police policies to ensure consistency, given that the PFCC's staff use communications equipment and technology issued by Essex Police, and are largely bound by its terms and conditions of employment.

8. Financial implications

There are no financial implications associated with this decision.

9. Legal implications

Adherence to the updated Use of Communications Policy attached at Appendix 1 should help to ensure adherence to relevant data protection and information security legislation and regulations.

10. Staffing implications

This policy applies to all persons granted access to the PFCC's or Essex Police's communication systems, including the PFCC, all permanent, temporary and agency staff, contractors and volunteers.

11. Equality and Diversity implications

The updated policy attached for approval at Appendix 1 is clear that:

 Those subject to its provisions must not use any PFCC or Essex Police provided facility to obtain, store, access or use any material considered to breach discrimination laws or any PFCC policies or procedures, or to contain any

[NOT PROTECTIVELY MARKED]

- offensive material. In the event that a user inadvertently accesses or receives such material, the policy requires them to inform their line manager and Essex Police's IT Service Desk immediately, in order that the problem can be looked into.
- The email system must never be used to create or send any material or other information which might be considered to be offensive, hostile, harassing, intimidating or disruptive, or which contains any form of profanity or which undermines the professional and ethical standards of the PFCC.
- Under no circumstances is an allocated mobile telephone to be used to convey any visual or audible message which could be considered to be offensive, obscene or menacing.

12. Risks

No risks have been identified in connection with this decision. The policy attached for approval at Appendix 1 requires users of mobile computing devices to receive a formal briefing on the additional risks and security measures associated with these, and to sign written security operating procedures, before being issued with such devices.

13. Governance Boards

The updated policy attached for approval at Appendix 1 was discussed at the PFCC's SMT on 14 April 2020 and approved in principal for adoption by the PFCC.

14. Background papers

Appendix 1 – Use of Communications Policy v5.0

[NOT PROTECTIVELY MARKED]

Report Approval

The report will be signed or review and sign off by the	•		Chief Exe	ecutive and T	reasure	r prior to
Chief Executive / M.O.		Sign:	Me Both			
		Print:	P. Brent-l	sherwood		
		Date:	14 April 2	020		
Chief Finance Officer / Tro	easurer	Sign:	Eh	olu		
		Print:	Elizabeth	Helm		
<u>Publication</u>		Date:	21 April 2	020		
Is the report for publicat		YES NO	X			
If 'NO', please give reasclassification of the docum		•	lication (nt, cite t	he security
If the report is not for publican be informed of the de	ication, th	N/A.				
Redaction						
If the report is for public	ation, is	redaction	on require	ed:		
1. Of Decision Sheet?	YES	2. Of Appendix? YES				
	NO	X			NO	X
If 'YES', please provide	details of	f require	ed redacti			
		N/A				

Date redaction carried out:

<u>Treasurer / Chief Executive Sign Off – for Redactions only</u>					
If redaction is required, the Treasurer or Chief Executive is to sign off that redaction has been completed.					
Sign:					
Print:					
Chief Executive/Treasurer					
Decision and Final Sign Off					
I agree the recommendations to this report:					
Sign:					
Print: Roger Hirst					
PFCC					
Date signed: 24 April 2020					
I do not agree the recommendations to this report because:					
Sign:					
Print:					
PECC/Denuty PECC					

Date signed: