POLICY – Cyber Protect

Number: S 4600  Date Published: 1 June 2017

1.0 Summary of Changes

1.1 This is a new joint policy for Essex Police and Kent Police. It should be read by all members of staff who are involved with Cyber Crime Prevention.

2.0 What this policy is about

2.1 This policy governs the response of Essex Police and Kent Police to the provision of Cyber Crime Prevention advice and support of the National Cyber Protect Network.

2.2 It predominately should be used by those working in the area of Cyber Protect, but also has applications on frontline officers dealing with the public for offences that have a Cyber or Digital element.

Compliance with this policy and any linked procedures is mandatory.

3.0 Statement of Policy

3.1 The application of this policy and its associated procedures will assist the forces to fulfil their obligations to support the National Cyber Protect Network.

3.2 The provision of Cyber Protect advice is part of the National 4P strategy and vital to the scale and nature of Cyber Crime.

3.3 The Policing Cyber Protect network is:

- The Economic and Cyber Crime Prevention Centre (ECPC) within the City of London Police;
- The Metropolitan Police;
- ROCU Cyber Protect Officers;
- Force Protect officers.

3.4 The role of the policing Cyber Protect network is to:

- Reduce the vulnerability of public, private and voluntary organisations by influencing protective security across their networks by providing coordinated, consistent and timely advice to those who are targeted by serious and organised crime, notably through cyber dependent and cyber-enabled crime;
- Make public, private and voluntary organisations more resilient against cyber-crime;
- Promote the cyber essentials programme for businesses;
- Reduce the vulnerability of individuals to cyber-crime through delivery of public awareness campaigns;
- Sharpen policing’s ability to identify the nature and attribution of cyber-attacks;
POLICY – Cyber Protect

Number: S 4600 Date Published: 1 June 2017

- Implement targeted public campaigns, issuing effective advice to business and local communities.
- Increase the reporting of cyber-crime to police, through Action Fraud, and the sharing of intelligence through the Cyber Information Sharing Platform (CiSP).

4.0 Implications of the Policy

4.1 Finance / Staffing / Training / Other

4.1.1 Implementation of the policy will require:

- **Estates:** Provision will be required for accommodation where there is an uplift in staffing or where there is the creation of a complete new department such as Cyber Crime;
- **Training:** The areas the forces are looking to invest in require significant investment in skills and training for both police officers and staff;
- **IT requirements:** Whilst some hardware such as desktops and laptops can be redistributed the software is bespoke and requires specific licences to cater for the unique type of investigation technique this policy covers.

4.2 Risk Assessment(s)

4.2.1 There is no specific risk assessment or health and safety consideration thought relevant to the content of this protocol.

4.2.2 Officers and members of police staff engaged within the process must remain aware that they must follow the protocol correctly otherwise the risk to the organisation of a possible civil action by members of the public. A failure to fully adopt the principles set out in this protocol could have a detrimental effect upon the reputation of the organisation.

4.3 Equality Impact Assessment

4.3.1 An Equality Impact Assessment has been carried out and shows the proposals in this policy would have no differential impact on the grounds of age, sex, disability, race, religion or belief, marriage and civil partnership, sexual orientation, gender reassignment and pregnancy and maternity.

5.0 Consultation

5.1 The following have been consulted during the formulation of this document:

- Unison
- Police Federation
6.0 Monitoring and Review

6.1 This policy will be reviewed by the Superintendent Serious Economic Crime Unit on behalf of the owner every year to ensure it remains fit for purpose and up to date.

7.0 Related force policies or related procedures (Essex) / linked standard operating procedures (Kent)

- S 1107 Procedure/SOP – Cyber Crime Unit

8.0 Other source documents, e.g. Legislation, APP, partnership agreements (if applicable)

None