OFFICE OF THE POLICE AND CRIME COMMISSIONER

INFORMATION SECURITY POLICY

Introduction

The OPCC recognises the importance of information assets and the need for proper, effective management of information systems, security safeguards and counter measures to protect information assets. This will be achieved by:

Maintaining appropriate security standards, specifically with HMG Security Policy Framework;
Ensuring the security of protectively marked & sensitive information and information assets both belonging to OPCC and entrusted to it by other organisations;
Ensuring all staff are aware of their responsibilities relating to the security of information and their duty to comply with Force policy and procedures relating to Information Security;
Meeting statutory obligations e.g. Data Protection Act (2018).

Information takes many forms and includes information stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes, CD/DVD, USB Memory Sticks, portable hard disk drives or spoken in conversation or over the telephone or airwave terminals.

The OPCCs' approach to information security is to balance the business requirements with the risk and potential impact of an information security breach, and the associated cost and logistics of implementing security controls.

Compliance

All personnel have an individual and collective responsibility to fully comply with the requirements of legislation pertaining to the protection of information including the security of information. Legislation includes but is not limited to:

Data Protection Act 2018
Human Rights Act 1998 & European Convention on Human Rights
Official Secrets Act 1989
Copyright Design & Patents Act 1998
Computer Misuse Act 1990
Electronic Communications Act 2000
Intercept of Communications Act 1985
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Wireless Telegraphy Act 1949
Crime & Disorder Act 1998
Criminal Procedure & Investigations Act 1996