INFORMATION SECURITY POLICY

CONTENTS

1.   INTRODUCTION

This Policy forms part of the Information Security Management System (ISMS) and sets out the policy and procedures to be followed by Staffordshire Fire and Rescue Service (SFRS) staff in order to keep SFRS information assets secure. The Information Security Policy should be read in conjunction with the other information security policies, these are listed below for reference:

Bring Your Own Device (BYOD) and Teleworking Policy
Business Continuity Management Policy Statement
CCTV, Video and Audio Surveillance Policy
Copying Copyright Material
Data Protection, Privacy and Confidentiality Policy
Freedom of Information Access, Publication and Re-use Policy
ICT Acceptable Use Policy
ICT Change Management Policy
Information Backup and Restore Policy
Password Management Policy
Record Retention and Disposal Policy
Security Classification Policy
Third Party Access (ICT Systems) Policy

2.   PURPOSE

Staffordshire Fire and Rescue Service's core purpose is to:

- Respond: Put out fires and rescue people
- Prevent and Protect: Do sensible things to prevent fires and incidents occurring.

The Service can only fulfil its duties if its employees have timely access to accurate information and this information is adequately protected against damage, tampering, theft, destruction and other threats. Stakeholders rely on the Service keeping information secure.

3.   DEFINITIONS

For the purposes of this policy, the following definitions apply:

Availability	The property of information being accessible and usable on demand by an authorised person.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, organisations or processes.
Consequence	The outcome of an event affecting objectives.
Data Protection Officer	Statutory officer under UKGDPR and Data Protection Act 2018 who oversees personal information and security, internal auditor and disclosure officer duties. The Data Protection Officer also oversees training and data breach / incident reporting and investigations.
IAO	Information Asset Owner, responsible for ensuring that specific information assets are handled and managed appropriately and that their value to the Service is not exploited.
Information security	The preservation of confidentiality, integrity and availability of information.
Integrity	An information asset's property of accuracy and completeness.
ITSO	IT Security Officer, responsible for applying technical controls to manage risk.
Likelihood	The chance of something happening.
Objective	A result to be achieved.
Policy	The intentions and direction of an organisation as formally expressed by its top management.
Risk	The effect of uncertainty on objectives.
Risk treatment	A process to modify risk.
SIRO	Senior Information Risk Owner, responsible for understanding how the strategic business goals of the organisation may be impacted by the use of the Service's information systems and data processing.
Stakeholder	A person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity.

Information Security Policy   Job No: 897   Issue Date: 09 June 2023   Page **2** of **5**

Any printed documents are considered uncontrolled. You must check with the current version on Staffnet.

4. INFORMATION SECURITY OBJECTIVES

The Service's information security objectives are to:

- Continually strive to reduce the incidence of adverse information security incidents

- Increase the awareness of employees in relation to good practice and current information security threats

- Comply with relevant legislation, for example: Public Records Act 1967, Copyright, Designs and Patents Act 1988, Official Secrets Act 1989, Computer Misuse Act 1990, Copyright (Computer Programs) Regulations 1992, Obscene Publications Act 1964, Data Protection Act 2018, Human Rights Act 1998, Freedom of Information Act 2000, Regulation of Investigatory Powers Act 2000, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, The Terrorism Act 2000, The Anti-Terrorism, Crime and Security Act 2001, Privacy and Electronic Communications Regulations 2003, Equality Act 2010, UK GDPR Guidance and Resources

- Ensure the Confidentiality, Integrity and Availability of information is maintained in line with its classification.

These objectives will be met through the Service's Information Security Management System (ISMS) based on ISO/IEC 27001:2017. Performance of the ISMS will be monitored against these objectives.

5. INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Post	Role	Duties
Deputy Chief Fire Officer	SIRO	Senior decision maker for risk and compliance with legislation and regulatory requirements.
Data Protection Officer	DPO	Oversees information and security compliance, staff awareness, approves information disclosure, policy creation and updating, advice and guidance.
Head of Property	IAO	Building security, waste disposal, utilities
Head of ICT	IAO	Security of IT hardware and software
Head of Personnel	IAO	Staff supply, vetting, training and discipline
Head of Emergency Response Team (ERT)	IAO	Data on resources of operational response, personnel and security of equipment and vehicles.
Head of Central Prevent and Protect (CPP)	IAO	Prevent and protect data
Head of Strategy and Intelligence Department (SID)	IAO	General management of systems and data under SID. Business continuity, response & incident data, risk management, insurance claims and complaints
Corporate Safety Planning Manager	IAO	Business Intelligence and HMICFRS data
Financial Services Manager	IAO	All finance data, anti-fraud measures
Head of Marketing and Communications	IAO	Security of social media, web site and marketing data.
Head of Learning & Development	IAO	Security of training data, operational assurance.
SDG Leads	IAO	Data held on stations, operational personnel and vehicles.
ICT Operations Manager	ITSO	Technical IT security controls
Head of Health and Safety	IAO	Security of Safety Event and DSE Data
Head of JETS	IAO	Security of Vehicle Data

6. RISK ASSESSMENT AND ACCEPTANCE CRITERIA

The Service's Strategic Risk Management System grades all risks on a scale of 1-16 using a 4 x 4, Impact x Likelihood matrix and risks scoring 8 or less after treatment are deemed to be acceptable. If a risk is assessed to be greater than this level, then suitable controls must be implemented so that the residual risk is within the accepted levels, ensuring that treatment of the risk, does not adversely impact the ability of employees to fulfil their duties or the effectiveness of other risk controls.

This policy will be reviewed regularly to ensure that it continues to be aligned with the Service's business objectives and to enable any opportunities for improvements to be incorporated. These reviews will be carried out by the Protective Security Steering Group, who will also be responsible for making decisions on any deviations or exceptions from this policy.

7. INCIDENT REPORTING

All employees must report information security events, whether resulting in an actual information security incident or not, to their Line Manager within 24 hours and the ICT helpdesk, so that they can

be passed to the Data Protection Officer. Incidents will be recorded by the DPO so that progress can be monitored and improvements implemented from any lessons learned. The DPO will also report on these incidents at the Protective Security Steering Group.

Consultation End Date: 06/07/2021			People Impact Assessed: 07/06/2021		Review Date: 19/08/2024	
Personnel may share the information in this document with members of the public:					Yes	
© Copyright: Staffordshire Commissioner (Fire and Rescue Authority)						
Date of Issue:	Title of Document:	Job No.:	Author:	Department:	Manager Approval:	Additional Information:
09/06/2023	Information Security Policy	897	David Morris	Data Protection Officer (SID)	Glynn Luznyj 09/06/2023	Amendments to Section 3, 5 & 7
19/08/2021	Information Security Policy	897	Andrea Jones	ICT	Howard Watts 18/08/2021	
04/02/2019	Information Security Policy	897	Andrea Jones	ICT	David Greensmith 01/02/2019	Hyperlinks added to introduction
20/07/2017	Information Security Policy	897	Andrea Jones	ICT	David Greensmith 20/07/2017	
21/07/2014	Information Security Policy	897	Tracey Merrington	ICT	David Greensmith 17/07/2014	
02/07/2014	Information Security Policy	897	Tracey Merrington	ICT		Consultation
27/05/2010	Information Security Policy	897	Sue Love	ICT		
23/04/2010	Information Security Policy	897	Sue Love	ICT		Consultation