Information Security Statement

Five Councils Partnership Information Security statement is to secure data, information and IT systems in a manner which complies with legislation and meets accepted best practice protecting it from unauthorised use, disclosure, or destruction. By implementing appropriate controls, we will ensure the continuity of our business operations and mitigate business damage in the event of a security incident.

Scope

This Information Security Statement applies to all members of the Five Councils Partnership data and information. Such information includes electronic data that is stored on computers, (or physical media such as backup tapes, CD's), transmitted across Council networks, sent by fax, printed out or written on paper or spoken in conversation. It applies to users of such information including employees, temporary staff and third parties with whom Five Councils Partnership contracts to provide services which may use such information. All employees are directly responsible for implementing and complying with this document.

Information within the Five Councils possession is classified as OFFICIAL by default and documented in the Five Councils Information Classification document.

Objective

The aim of information security at Five Councils is to ensure:

- Confidentiality – information is accessible only to those authorised for access
- Integrity – information is accurate, up to date and/or in line with appropriate retention schedules and complete including all processing methods
- Availability – authorised users can have access to information when required.

It is our responsibility to ensure that:

- all customer data and or information is appropriately protected and is not divulged to any third party without authorisation
- suitable physical security and environmental controls are in place to protect the premises and,
- appropriate, access is restricted to authorised staff
- access to Council data and information is appropriately controlled
- all in house systems development is appropriately controlled and tested before live implementation
- all staff are provided with training in information security awareness and individual responsibilities defined.

Breaches

All data and security breaches, actual or suspected, must be reported to the Councils Data Protection Officer immediately, who will ensure they are investigated in accordance with the Data Breach Policy. Breaches of this document and or associated policies will be referred to the Councils disciplinary policy and may result in termination of employment and or legal action / prosecution.

Ownership and Maintenance

This document is owned and maintained by the 5C Security Working Group.
The Senior Information Risk Owner approves this document.

Signed:  Date: 3 Oct 2022

Matt Goodwin, SIRO, Havant BC