SOUTH HOLLAND DISTRICT COUNCIL

Report of: **Executive Member for Governance and Customer, Tracey Carter**

To: **Policy Development Panel, 21 January 2020**

Author: **Sarah Barsby, Shared Executive Manager for Information**

Subject: **Information Security Framework and Policies**

Purpose: **To seek member feedback and comments on a new Information Security Framework which aims to ensure that a robust and secure ICT service is provided to the Council through its delivery partner PSPS.**

Recommendation(s):

1) That the contents of the report, together with the attached Information Security Framework, be noted and that comments and feedback – with particular regard to the Incident Management Procedure and the ICT Policies because they apply to SHDC officers and Members – be provided.

1.0 BACKGROUND

1.1 A review of the Council's ICT policies has been undertaken by PSPS, as part of its provision of ICT services and support to the Council, and taking into account feedback from a GDPR audit performed for PSPS in 2017 and subsequent Council audits performed in 2018.

1.2 Feedback received from these audits indicated that the policies were confusing to the reader and did not cover the range of policies that would be expected from a maturing ICT department such as that provided to the Council by PSPS.

1.3 In response, a project commenced to review and rewrite the Council's existing ICT policies and to encompass these within a new Information Security Framework (see Appendix A).

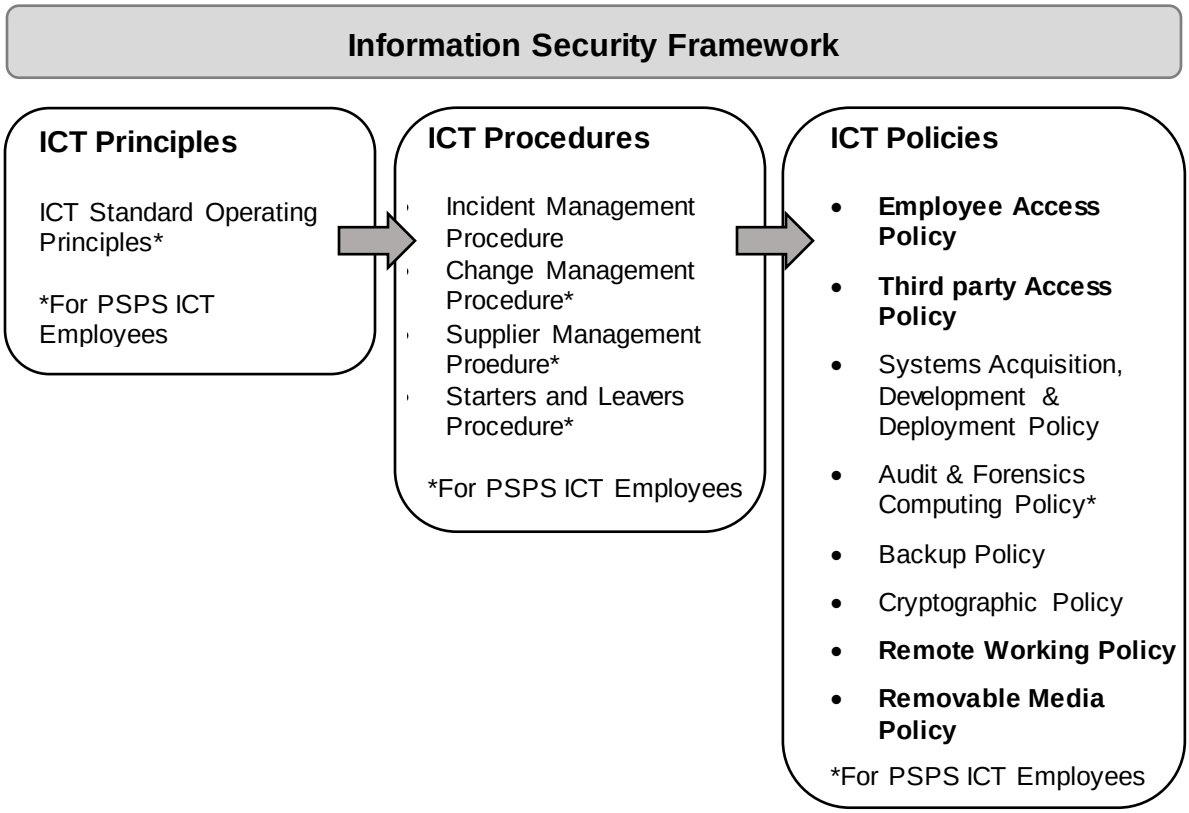
1.4 Having consulted with the Council's Member ICT Working Group in 2019, the document is presented to the Policy Development Panel today for wider member discussion and feedback, which will be considered by the Executive Member for Governance and Customer ahead of their final approval of the document.

2.0 Information Security Framework overview

2.1 The Information Security Framework is more than just a set of policies; it also includes procedures (both for PSPS ICT employees and for SHDC officers and Members) and underlying ICT principles for the ICT Service to adhere to, as part of its ongoing commitment to providing information security.

2.2 The following diagram sets out the principles, procedures and policies that form part of the Information Security Framework:

Diagram A – Information Security Framework structure



2.3 **ICT Principles:** Adopted by the ICT Service provided to the Council by PSPS, these principles underpin the technical work of the team and create a common standard for consistent and robust ICT service delivery.

2.4 **ICT Procedures**: These procedures are a mix of internal (for PSPS ICT employees) and external (for SHDC officers and elected Members) documents that offer step-by-step guidelines for certain re-occurring tasks, to make sure the Council is being consistent in its approach to ICT issues management and task completion.

2.5 **ICT Policies:** These Policies set out guiding principles for the use of ICT across the Council. Not all policies will apply to all users, however.

These policies can be further split into ICT-related policies (ie: technical policies that determine underlying infrastructure considerations) and policies which have a direct impact on SHDC officers and Members (highlighted in bold text, in diagram A above).

2.6 This report seeks feedback on the framework; in particular, the Incident Management Procedure and the Employee Access Policy, because they apply to SHDC Members, as well as officers.

3.0 Policies review

3.1 Currently, the Council has 14 policies which make up an ICT 'Information Set'. To streamline and improve readability, these policies have been reviewed as follows:

Current Policies	2020 Policies update
Communications & Operation Management	RETIRED – now included in the ICT Standard Operating Procedure
Computer, telephone and desk use	RETIRED – Covered in the Employee Access Policy
Email	RETIRED - Covered in the Employee Access Policy
Employee Information Security	RETIRED - Covered in the Employee Access Policy
GCSx Acceptable usage	RETIRED
Information Protection	RETIRED – duplication of Data Protection Policy
Information Security Incident Management	Reviewed & updated
Internet Acceptable Usage	RETIRED – covered in Employee Access Policy
IT Access	RETIRED – covered in Employee Access Policy
IT Infrastructure	RETIRED– now included in ICT Standard Operating Procedure
Legal Responsibilities	RETIRED – duplication of Data Protection Policy
Remote Working	Reviewed & updated
Removable Media	Reviewed & updated
Software Policy	RETIRED – covered in Systems Acquisition, Development & Deployment Policy

3.2 So, in summary the proposed new Information Security Framework now consists of eight policies, of which four are new:

- Employee* Access Policy (*covering elected Members, as well as officers)
- ICT Incident Management Procedure
- Remote Working Policy
- Removable Media Policy
- Third Party Access Policy (New)
- Systems Acquisition, Development and Deployment Policy (New)
- Audit & Forensics Policy (New)
- Cryptographic Policy (New)

A summary of each of the policies and its key features can be found in Appendix B of this report.

4.0 Impact on employees and elected Members

4.1 All SHDC staff will be required to read the appropriate new policies (this may be a subset of the Information Security Framework, dependant on role) and complete a short online assessment to prove they have understood them. This process will be completed on joining the Council and every two years thereafter.

4.2 Similarly, all Councillors will be required to read the new Employee Access Policy and ICT Incident Management Procedure and sign an acceptance form, as these documents apply to elected Members as well as officers.

4.3 It is anticipated that Councillors will sign the acceptance form at the ICT induction following a district council election and thereafter at major review only. However, as a

district election has only just taken place it is suggested that Members be asked to sign an acceptance form – either digitally, or before/after an upcoming meeting of Full Council (date to be agreed).

5.0 Framework review

5.1 Subject to Portfolio Holder sign-off, the Information Security Framework has been approved in principle by the Council's ICT and Customer Governance Board.

5.2 The draft framework has also been discussed by the ICT Member Working Group, where it was agreed that it should come forward to the Policy Development Panel for information and comments ahead of portfolio holder approval being granted.

6.0 OPTIONS

6.1 Note the contents of this report, together with the attached Information Security Framework, and provide comments and feedback – with particular regard to the Incident Management Procedure and the ICT Policies because they apply to SHDC officers and Members.

6.2 Do nothing.

7.0 REASONS FOR RECOMMENDATION(S)

7.1 Adopting this Framework – in particular, its set of ICT Policies – will provide greater clarity, with the reduction from 14 policies to eight further helping to focus Members and officers on the key issues and points contained within the policies themselves.

7.2 The new Framework takes account of the latest guidance and best practice regarding information security and data protection. This includes helping the Council to meet its obligations under GDPR (General Data Protection Regulation) legislation.

8.0 EXPECTED BENEFITS

8.1 With a streamlined, simplified and updated 'family' of policies, Members and officers will be better placed to know which policy/policies should be referred to for clarifying key ICT matters – such as incident management and remote working. In addition, a smaller set of policies will be easier to maintain and keep up-to-date.

8.2 The new Framework will help the Council to meet its requirements to keep data and the systems within which it is contained, as safe and secure as possible – helping to guard against major ICT incidents, such as cyber attacks.

9.0 IMPLICATIONS

In preparing this report, the report author has considered the likely implications of the decision - particularly in terms of Carbon Footprint / Environmental Issues; Constitutional & Legal; Contracts; Corporate Priorities; Crime & Disorder; Equality & Diversity/Human Rights; Financial; Health & Wellbeing; Reputation; Risk Management; Safeguarding; Staffing; Stakeholders/Consultation/Timescales; Transformation Programme; Other. Where the report author considers that there may be implications under one or more of these headings, these are identified below.

9.2 Constitution & Legal

The Information Security Framework sits outside of the core policy framework for the Council. Consequently, any decision concerning the adoption of a new or revised framework is an Executive Decision.

Major revisions of the Information Security Framework would be presented to PDP for information and comment, as part of any wider formal decision making process, and in liaison with the Portfolio Holder. The next scheduled review is due to take place in 2021.

Any minor changes required to the Framework would be approved by the Executive Manager for Information, following consultation with the ICT and Customer Governance Board.

9.3 Corporate Priorities

The proposed Information Security Framework supports the Council's key priorities of ensuring that our services are digitally enabled, efficient and meet the expectations of our changing community; and to continue to ensure that our regulatory and statutory services remain fully compliant with all current and emerging legislation.

5.7 Risk Management

Failure to adopt a new Information Security Framework that supports best practice in ICT systems and data management presents both an operational and reputational risk to the Council.

6.0 WARDS/COMMUNITIES AFFECTED

The Information Security Framework set out in this report will help to ensure secure and efficient service delivery and customer access, through well-managed ICT systems, that will benefit all wards/communities.

7.0 ACRONYMS

SHDC – South Holland District Council
PSPS – Public Sector Partnership Services Ltd

Background papers:-	None

Lead Contact Officer

Name and Post:	Sarah Barsby, Executive Manager for Information
Telephone Number:	07870 157290
Email:	sarah.barsby@breckland-sholland.gov.uk

Key Decision: No
Exempt Decision: No

This report refers to a Mandatory & Discretionary Service

Appendices attached to this report:

Appendix A	Draft Information Security Framework
Appendix B	Information Security Framework Policies – key features