APPENDIX

ACTION PLAN FOR IT ACCEPTABLE USAGE POLICY 2021/22

Rec Ref.	Rec No.	Recommendation	Rec Rating	Proposed Management Action	Lead Officer	Date to be Actioned	Comments for Audit Report
1.1	1	All guidance and policy documents relating to the acceptable use of IT facilities and systems should be reviewed. Consideration should be given to consolidating these into one policy and cross-referencing other policy documents that underpin the acceptable usage policy. They should be published to all users. User training materials should reflect these changes and users should be asked to confirm formally that they have read and understood what is required of them.	Significant	The appropriate policies will be reviewed and consideration will be given as to the consolidation of the policies into a more easily consumed format. Methods to enforce acknowledgement and understanding will also be considered.	Tim Collard Tim Collard	December 2022 December 2022	Progress is now being made towards a review of all guidance and policy documents relating to Information Governance and Security. An over-arching Information Governance Framework is being developed which will provide the context for all policies and guidance in this area.
1.2	2	A reminder should be issued to all staff on the location of the IT Acceptable Usage Policy.	Requires Attention	Agreed.	Tim Collard	December 2022	Confirm completion

1.3	3	In light of the refocus programme and the new hybrid approach to working, the Mobile and Remote Working Policy should be reviewed to ensure that the home working environment is fully considered and that the practicalities of mixing home and work life are detailed within it.	Requires Attention	The current policy is a security policy and the bulk of it is still applicable. This will be reviewed for security considerations as the Refocus and other programmes develop. Where guidance from HR is required, this will be considered.	Tim Collard	December 2022	An initial review has been undertaken but will be reviewed further once the Information Governance Framework has been completed
2.1	4	A reminder should be issued to all Council users on the procedures to follow in the event of a potential breach of acceptable use policies and guidance	Requires Attention	Agreed.	Tim Collard	December 2022	Confirm completion
3.1	5	All logs should be collated into a single Security Information and Event Management (SIEM) system, which can then process logs in near real time and create alerts for anomalies as soon as possible. Procedures should be created for the ongoing management and monitoring along with a formal review of the protective monitoring policy which is overdue by more than one year.	Significant	Funding for such a system in not identified, however SIEM products will be investigated and a business case produced to support any procurement if agreed to proceed.	Ian Churms/Chris Warrender	June 2022	The Council is currently trialling a third-party service which is proving of great value. A decision around a long-term investment will be taken in the new year

3.2	6	Intranet guidance regarding information security incident reporting should be reviewed and updated	Requires Attention	Agreed	Tim Collard	June 2022	This is being updated and will be completed once the Ivanti Information Security reporting process is in place.

ACTION PLAN FOR INFORMATION SECURITY MANAGEMENT 2021/22

Rec Ref.	Rec No.	Recommendation	Rec Rating	Proposed Management Action	Lead Officer	Date to be Actioned	Comments for Audit Report
2.1	2	The authority should have a suitably qualified Information Governance Officer/CISO in place as soon as possible in order to ensure that an appropriate information security governance framework is developed and managed.	Significant	The issue regarding the appropriate resourcing/skillset requirements for Information Governance and the development of a security framework will be raised with James Walton SIRO	Tim Collard	Early 2022	The authority has a qualified Data Protection Officer/Information Governance Officer in place. It is envisaged that Information Security generally will be the responsibility of the new Head of Governance role to which will be appointed to shortly. In the meantime, the

							responsibilities are split between IG and IT Security. The Information Security Strategy will sit under the Information Governance Framework.
2.2	3	The structure and purpose of the information security and governance groups should be revisited and terms of referenced produced for each. In relation to the steering group, currently the Information Governance Group, this should include the overseeing of the actions of the working group, currently the ISIGIT group. In addition, there should be a clear trail of actions agreed at the working group from the agenda through to the actions list. The interrelationship and referencing of items carried forward to actions should therefore be revisited. Ideally more formal minutes should be maintained as currently there is no record of the discussions for each topic on the agenda.	Significant	Done and continued to be worked on. ToR in place for security group and drafted for the IGG group	James Walton (SIRO)	Completed subject to IGG approval in January 2022	

4.1	5	The council, as part of its Information Governance process develop a data centric risk analysis and an information governance strategy alongside an overall cybersecurity strategy. This will allow the council to determine the appropriate level of security controls required and/or relied upon for its key data assets.	Requires Attention	The use of data risk mechanisms and analysis together with the development of an information governance strategy will be raised with James Walton, SIRO.	Tim Collard	June 2022	An Information Governance Risk Register has been commenced. Information Governance Strategy is being developed (as above). A new cyber strategy Is being created with the new Head of Automation and Technology alongside continuing technical and financial investment in this area.
5.1	6	The roles of Information Governance and ICT in the creation of O365 Data Loss Prevention Policies (DLP) and investigation of DLP non compliances should be defined and agreed by all parties. Once agreed the configuration of the current DLP policies should be completed. In addition, the O365 data scanning tools available under the E5 agreement should be used to identify and label any sensitive data stored within the file storage systems	Requires Attention	The development of further DLP policies and the use of O365 tools is a medium-term goal. This however is reliant on the available resource being in place to both develop the policies and to evaluate their impact. In the short term the process for	Tim Collard	June 2022	IG and ICT Security are considering ways of using DLP to i) reduce the number of security incidents, ii) monitor email traffic to check use of appropriate security controls when sending personal and financial information and iii) help to raise awareness of users of email services.

				monitoring noncompliance with existing deployed DLP policies will be determined and implemented. The overall approach to DLP will be raised within the within the IGIT group and an action plan developed.			
9.1	8	There should be some form of summary record maintained of incidents, the template produced in January 2021 would seem a reasonable starting point, although it should also include a reference to the investigation files. The Information Governance Group should specify their incident reporting information requirements in order to maximise the benefit of lessons learned across the organisation.	Requires Attention	The requirement for reporting to IGG will be discussed at the next IGG group so that appropriate, meaningful and accurate reporting can be provided. IG / IS will amend the recording and collation as required to meet the reporting needs of IGG	Ian Churms	Early 2022	Incident Management is being reviewed. IG and IT are considering a single reporting tool where all Security Incidents, Cyber Incidents and Personal Data Breaches can be recorded in one place. This will enable several teams to work more easily together where breaches need a response from multiple teams, eg cyber incident resulting in personal data being compromised. This will enable better reporting to

							be provided to management teams so that underlying causes and new vulnerabilities can be identified and treated early