Audit & Standards committee – 9 February 2018
Supplementary report – Agreed Action Plans

General Data Protection Regulations implementation arrangements **Item number 8**

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
1.	<u>Implementation plan</u> Strategy Group should ensure that a work plan together with detailed action(s) is put in place to track progress for each of the GDPR work streams. Actions should be allocated to lead officers. Work plan should include requirement to update policies, procedures and other governance documents. In line with the requirements a Data Protection Officer should be appointed. **Note:** This does not need to be a dedicated role.	Medium	An Information Governance group is to be initiated. Progress will be regularly reported to Strategy Group. To be appointed.	ACE (Business Support) ACE (Business Support)	November 2017 and on-going May 2018

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

Audit & Standards committee – 9 February 2018
Supplementary report – Agreed Action Plans

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
2.	Training Training in relation to GDPR should be refreshed and updated in conjunction with implementation of new/updated policies and procedures. Temporary staff should also be provided with training. There should be regular and proportionate data protection refresher training for staff that have access to personal data. Staff should provide positive attestation for training provided. **Note:** An e-training tool would allow timely refresher training or induction training, serve as reference resource and provide positive self-assessment attestation.	Medium	Training has been provided to all staff. e-training (audio-visual media) will be provided via intranet and as part of training plans.	Senior Legal Advisor	November 2017 and on-going

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

Audit & Standards committee – 9 February 2018
Supplementary report – Agreed Action Plans

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
3.	3rd Parties In compliance with the GDPR, current arrangements should be reviewed to ensure SPT has contract(s) in place with any third party who processes or has access to personal data on SPT's behalf. Management should be satisfied that • third parties provide sufficient guarantees about security measures implemented to protect any personal data and its' processing; • take reasonable steps to check that those security measures are put into practice; • have a written contract setting out what the third party is allowed to do with the personal data including security measures e.g. o technical security controls including encryption and endpoint control to prevent unauthorised uploading or downloading of information; o System access and password requirements; o Storage of manual records and locked screens o Fair processing, including CCTV o Retention of personal data, etc.	High	Information Governance group to review 3rd party arrangements.	Information Governance group	November 2017 and on-going

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
	Note: Contract terms and conditions to include GDPR requirements.				
4.	<u>Consent</u> Management should review how SPT seek(s), obtain(s) and record(s) consent for processing personal data. Consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent has to be verifiable. An audit trail of any consent should be maintained. Liaison with partners/contractors should be recorded to ensure GDPR requirements are met. **Note:** particular cognise should be given to children's and vulnerable persons' data. Consent forms may be required for ticketing applications and travel arrangements.	High	Consent for all types of information provision to be reviewed. Website consent options being explored.	Senior Legal Advisor/ Digital manager	November 2017 and on-going

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

Audit & Standards committee – 9 February 2018
Supplementary report – Agreed Action Plans

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
5.	Data breach Management should review procedures and practices in place to ensure data breaches can be detected, reported and investigated timeously. **Note:** A notifiable breach has to be reported to the Information Commissioners Office (ICO) within 72 hours of the organisation becoming aware of it. Not all breaches will have to be notified to the ICO, only ones where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows for provision of information in phases. If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay. Failing to notify a breach when required to do so can result in a significant fine.	High	Procedures for reporting breaches to be reviewed (by Information governance group). Awareness of new procedure to be raised via internet.	Senior Legal Advisor	November 2017 and on-going

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

Audit & Standards committee – 9 February 2018
Supplementary report – Agreed Action Plans

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
6.	Subject Access Requests (SAR) The current SAR process should be reviewed to ensure compliance with GDPR. The resultant procedures should be documented and provided to all relevant staff for adherence. The documented procedures should include the following: • process for receiving and allocating SAR requests; • requirements including eligibility checks; • forms to be completed; and • record keeping requirements including recording of timescales (e.g. request date, response date), refusals, and multiple requests by same body/individual, any charge levied. **Note:** A digital solution should be sought for record keeping this would have the advantage of providing a dedicated web based SAR customer interfacing and a centralised log.	Medium	Process to be reviewed and centralised to enhance arrangements.	Senior Legal Advisor	November 2017 and on-going

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

Audit & Standards committee – 9 February 2018
Supplementary report – Agreed Action Plans

Core financial system review of expenses **Item number 10**

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
1.	<u>Expenses paid via payroll to staff</u> Finance management should not process expense claims that are not fully completed in accordance with prescribed guidance.	Low	Expense claims that are not fully compliant with the prescribed guidance will not be processed.	Chief Accountant	Implemented
2.	<u>Imprest/petty cash holding</u> Finance management should re-issue guidance to all designated imprest/petty cash holders on the following issues: • reimbursement period should not exceed 3 months; • receipts should accompany all expenditure lines; • reimbursement for travel and subsistence should not be processed using imprest/petty cash. Staff should process claims via payroll.	Medium	Procedural guidance will be reviewed and re-issued to all imprest/petty cash holders. This review will be supplemented by a training session(s) where required.	Chief Accountant	January 2018

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

Audit & Standards committee – 9 February 2018
Supplementary report – Agreed Action Plans

Systems review of MyBus administration **Item number 11**

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
1.	Procedural guidance Bus Services management should review/update/enhance procedural guidance for MyBus call handling and use of the digital system.	Medium	Current procedural guidance and basic script provided to train/support MyBus dispatchers will be reviewed and enhanced.	Demand Responsive Transport (DRT) Team Leader	March 2018
2.	Standing data Bus Services management should undertake a data cleansing exercise on standing data held in accordance with records retention schedules.	Medium	Bus Services management will liaise with Digital and Legal services to undertake a data cleansing exercise.	Bus Services Manager / DRT Team Leader	March 2018
3.	MyBus call records Bus Services management should undertake a data cleansing exercise of telephone call (audio) records held in accordance with retention schedules.	Medium	Bus Services management will liaise with Digital and Legal services to undertake a data cleansing exercise.	Bus Services Manager / DRT Team Leader	March 2018
4.	System access Bus Services management should obtain a report from the digital system to confirm the authorised system users and permissions, and where appropriate, undertake a data cleansing exercise.	High	The digital system administrator will liaise with the external service provider to develop access reporting and where appropriate undertake a data cleansing exercise.	DRT Team Leader	March 2018

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

Audit & Standards committee – 9 February 2018
Supplementary report – Agreed Action Plans

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
5.	Contract management Bus Services management should review the current system for contractual non-compliance (penalties) applied to MyBus service provision.	Medium	A short-life working group has been set up to review the contractual non-compliance (complaints, warnings and appeals) process. This group includes representatives from Digital and Legal services.	Bus Services Manager	March 2018
6.	Contract management Bus Services management should review the process for applying financial penalties for contractual breaches by bus operators for MyBus service provision.	Medium	A short-life working group has been set up to review the contractual non-compliance (complaints, warnings and appeals) process. This group includes representatives from Digital and Legal services.	Bus Services Manager	March 2018
7.	Fares Bus Services management should review the accuracy and currency of the MyBus fares guideline criteria.	Medium	The MyBus and MyBus Rural fares guideline criteria will be reviewed. Any proposed change to the maximum permitted fare scale will require Strategy Group and Committee approval.	Bus Services Manager	March 2018

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

Audit & Standards committee – 9 February 2018
Supplementary report – Agreed Action Plans

Digital controls review of Social Media **Item number 12**

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
1.	<u>Policy and procedures</u> Digital (IT) policies and procedures should be reviewed and enhanced to incorporate Social Media administration.	High	Agreed.	Digital Manager	April 2018
2.	<u>Social Media strategy</u> The draft Communications plan 2017/18 and Social Media Strategy (May 2017 (v0.4)) should be reviewed and finalised. A Crisis Communication Strategy should be incorporated in these documents. Strategy documentation should be complementary and be aligned to SPT's vision and objectives. The finalised documents should then be presented to the Strategy Group for their review and authorisation. Separate operational guidance for staff (including access controls to Social Media accounts, moderation procedure, escalation process, absence cover arrangements etc.) should be available.	High	Agreed.	Digital Manager and Media & Public Affairs Manager	April 2018

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
	This could serve as a Digital staff training document. **Note:** Any employee who has responsibility for any aspect of the Social Media should be trained on access controls, use of relevant platforms as well as the policy around moderation and posting.				
3.	<u>Social Media breaches</u> A record of Social Media incidents/breaches should be maintained. **Note:** a low incident rate could help provide management with positive assurance on performance.	Medium	Agreed, a record will be maintained. **Note:** a corporate digital solution will be implemented by October 2018.	Digital Manager	December 2017
4.	<u>Performance information</u> The Communications and Social Media Strategy should outline specific, measureable, achievable, realistic and time bound (SMART) performance indicators.	Medium	Agreed.	Digital Manager	April 2018

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
	Senior management should receive reports on the following information: • Organisational requirements; • Who is using Social Media, for what and why; • When they are using it or in response to; • What influence/outcome (obtained); • How return on investment for campaigns is evaluated; • Engagement levels based on population using service (in addition to change from previous month). The reporting lines, exception reporting outwith tolerances should be considered.				

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.

Audit & Standards committee – 9 February 2018
Supplementary report – Agreed Action Plans

Digital controls review of cyber resilience arrangements **Item number 13**

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
1.	Cyber Resilience Public Sector Action Plan To ensure compliance and adherence with the timelines set in the Scottish Government Cyber Resilience Public Sector Action Plan. In addition, progress should be regularly reported to Strategy Group.	High	Agreed, Strategy Group will receive regular updates on action plan.	Digital Manager	Scottish Government milestones: 31 March 2018; 30 June 2018 and 31 October 2018

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.