Organisation	**St Giles Trust**
Title	**ISMS and Data Protection Policy**
Author	**Data Protection Team**
Owner	**Assistant Chief Executive**
Subject	**ISO 27001**
Protective Marking	**Official**
Review date	**Nov 2023**

INFORMATION SECURITY POLICY

Information security is defined as "*the protection of information against unauthorised disclosure, transfer, modification, or destruction, whether accidental or intentional*"[1]. This document sets out St Giles Trust's (SGT) commitment to maintaining the information security principles of confidentially, availability and integrity on all information we hold - about clients, our own information and on the systems we use - and all our processes in accordance with internationally recognised standards and relevant legal requirements, for example the Data Protection Act 2018, UK GDPR and ISO27001 (the international standard for Information Security). This is critical to helping clients and the on-going success, functioning and good governance of the charity. Failure to adequately secure information increases risks to clients' wellbeing and the risk of financial and reputational losses, from which it may be difficult for the charity to recover.

This document and our other information security policies, guidelines and processes make up our Information Security Management System (ISMS) and it applies to all our business processes. Although we make use of sophisticated technology to enforce and apply policies, the goal to keep information secure and make continual improvements to effectively manage new opportunities and threats, requires the concerted effort of **everyone** to 'do their part' and result in us having an effective ISMS.

This document contains our Information Security Policy that provides the guiding principles and responsibilities necessary to safeguard information and systems and the framework for an effective ISMS. It has an overview of our management direction and support of Information Security in accordance with business requirements, legal requirements and contractual obligations. Meeting Data Protection requirements is a key requirement of information security for us, so this document also contains details of how we do this, see Appendix 1.

We require all employees and the third parties that work for us, to adhere to the ISMS and communicate them to others so we can achieve our commitments to satisfy applicable requirements related to information security and to establish, implement, maintain and continually improve the ISMS across our processes. We make key documents available to interested parties so they are aware of our commitment to information security and also aware of any security obligations they have to us.

We have an ISMS Steering Committee responsible for managing ISMS tasks and reporting on information security performance to Trustees and the Senior Management Team. The Assistant Chief Executive is the Chair, and also has the role of 'Information Security Manager' within the ISMS. The other core members are the Data Protection Team. The chair and core members have the authority to take actions to ensure the ISMS meets the requirements of ISO27001:2017. The Data Protection Team are the main contact point for any questions about information security and data protection Dataprotection@StGilesTrust.org.uk. The latest version of policies, guidelines and procedures are available on Atlas.

Malcolm Walker
Assistant Chief Executive and Finance Director

[1] https://electropedia.org/iev/iev.nsf/display?openform&ievref=721-08-57

1.0 POLICY OBJECTIVES

- To direct the design, implementation and management of an effective ISMS which takes into account information security requirements of key interested parties and ensures SGT information assets are properly identified and recorded, and afforded suitable protection at all times.

- To ensure the confidentiality, integrity and availability of SGT's information assets, and supporting assets (including information systems) as defined within the Inventory of Assets.

- To ensure that all vulnerabilities, threats and risks to information assets and supporting assets are formally identified, understood, assessed and controlled in accordance with SGT's documented Risk Assessment and Risk Management Procedure.

- To ensure that SGT employees[3], contractors and third party users comply with this Information Security Policy (aka ISMS policy), and all other ISMS documentation, through the provision of effective information security training, awareness and ongoing monitoring activities.

- To ensure that SGT is able to maintain full compliance with all applicable legislation, regulations and contractual requirements, and any supporting management system certifications.

1.1 Organisation objectives for the ISMS

The Senior Management Team (SMT) have defined the following objectives for the ISMS so business strategy and requirements from regulations, legislation and contracts are met:

- Protect the confidentiality, integrity and availability of information assets (**OBJ-01**)
- Ensure all employees and partners are aware of the SGT ISMS and way of working (**OBJ-02**)
- Comply with all relevant legislation and regulations to information security, especially data protection requirements (**OBJ-03**)
- Meet the contractual requirements of funders and potential funders[4] (**OBJ-04**)

The KPIs in the table below are agreed by the ISMS Steering Committee to determine if the organisation objectives. KPI reports will be generated on a monthly basis by the Data Protection Team, see St Giles Trust Information Security KPIs for details on how they are measured.

KPIs	Organisation Objectives			
	OBJ-01	OBJ-02	OBJ-03	OBJ-04
Training and awareness - 80% of staff are aware of the ISMS policy and their responsibilities for doing work according to procedures, reporting incidents etc.	✓	✓	✓	✓
Internal audits - 100% of scheduled internal audits completed within 1 month of target date	✓		✓	

[3] Employees includes volunteers
[4] Limited to potential funders where requirements are achievable and do not compromise existing funder requirements

KPIs	Organisation Objectives			
	OBJ-01	OBJ-02	OBJ-03	OBJ-04
Data Protection Impact Assessments for Projects – done within 2 months of project going onto live section of spreadsheet	✓	✓	✓	✓
Incidents - 100% of suspected or actual data breaches, losses of mobiles, laptops or paper records reported and any other information security incident within 24 hours	✓		✓	✓
Physical asset register – has been updated/reviewed within the past 90 days	✓		✓	
Meeting Retention requirements for personal data – all types of personal data (paper and electronic) deleted when there is no lawful basis for processing it – excluding emails	✓		✓	✓

2.0 POLICY SCOPE

St Giles Trust shows people there is a way to build a better future – for themselves and those they care about – and help them create this through support, advice and training. The Information Security Management System covers the delivery of services assisting people who have been held back by poverty, exploitation, abuse, addiction, mental health problems, caught up in crime or a combination of these issues and others within the UK.

Locations with the scope of the ISMS
St Giles Trust Head Office: 64-68 Camberwell Church Street London SE5 8JB
St Giles North London: Resources for London 356 Holloway Road London N7 6PA
St Giles Trust Cymru Unit 8 Coopers Yard Curran Road Cardiff CF10 5NB
St Giles Trust Yorkshire Leeds Media Centre, 21 Saville Mount, Leeds LS7 3HZ
St Giles Trust West London (K&C) Office 3, 1 Thorpe Close, London, W10 5XL
St Giles Trust Wrexham, 14 Grosvenor Road, Wrexham LL11 1BU
St Giles Trust Midlands, 3 Castle Yard, Coventry, CV1 5RF
St Giles Pantry 62 Camberwell Church Street SE58JB
St Giles Norwich St Saviours Church, Magdalen Street, Norwich, Norfolk NR3 1AA
St Giles Swansea, Unit 9 Orchard House, 7 Orchard Street Swansea SA1 5AS
St Giles Newport, Offices 24/25 The Orion Suite, Enterprise Way, Newport NP20 2DX
St Giles Wolverhampton, St David's Court, Union Street, Wolverhampton, West Midlands, WV1 3JE
St Giles York, 3 Odeon Buildings, Blossom St, York YO24 1AJ

The key interested parties for the ISMS, and their main information security requirements, are shown in Appendix 1.

Information stored in prisons, and the way work is done within prisons, is outside of the scope of this policy.

SGT's Information Security Policy shall include the following:

❖ 2.1 Information Assets

All information assets (data) either owned by SGT or entrusted to SGT by a client or a partner/third party under an agreement which specifically details SGT responsibility for that data, and including:

- Information assets held, processed or stored on SGT premises
- Information assets held, processed or stored at approved off-site premises or locations

❖ 2.2 Supporting Assets

All supporting assets (non-data) which by direct or indirect association are an integral part of ensuring the confidentiality, integrity or availability of the information assets described in Section 2.1, including:

- Premises (including offices, data centres, storage facilities, recovery sites etc.)
- Hardware (including servers, network infrastructure, laptop computers, desktop computers, storage infrastructure and mobile devices)
- Software (including operating systems and commercially available software applications)
- SGT personnel (including permanent, temporary, full-time and part-time employees, authorised contractors and any third party users of information systems)

❖ 2.3 Documentation and Records

All policies, processes, procedures, work instructions and records related to the management, use, control and disposal of the information assets and their supporting assets detailed above.

3.0 POLICY STATEMENTS

SGT shall be committed to the protection of the information assets and supporting assets as defined within the Scope of this Policy. SGT has created its ISMS in accordance with the international Information Security Management Systems standard ISO/IEC 27001:2017 this framework shall be followed for all information security related activities, and SGT shall seek to retain external certification against this standard.

To effectively manage and deliver its ISMS, SGT shall:

❖ 3.1 Inventory of Assets

Define and maintain a comprehensive Inventory of Assets, including all information assets and supporting assets as defined within Section 2.0 of this Policy. The Inventory of Assets shall detail a named owner for each asset, who shall fully understand their responsibilities for the protection of the asset.

To ensure compliance with the GDPR, SGT will maintain an accurate and up to date register of all electronic and physical data assets containing personal data.

❖ 3.2 Access Control Policy

Ensure that all information assets, and their supporting assets, are protected so as to ensure their confidentiality, integrity and availability is maintained. Access to information assets and supporting assets shall be in accordance with SGT's Access Control Policy, and be restricted to the minimum required to undertake authorised business activities, and SGT has adopted the principle that "access is forbidden unless it has been specifically and formally pre-authorised".

❖ 3.3 Information Classification and Handling

Ensure that all information assets shall be classified and handled in accordance with the SGT Classification and Handling Procedure, which details how information assets of different sensitivities shall be managed, handled, processed, encrypted/protected, stored, transmitted, dispatched and disposed of when no longer required.

❖ 3.4 Acceptable Use

Ensure that all personnel, contractors and third party users comply with the SGT Acceptable Use Policy which details how information assets and their supporting assets should be used in an acceptable manner and in accordance with all ISMS related policies and processes. This policy shall detail the acceptable methods of use of information processing systems, networks (including, for example, the internet and telephone systems) and other resources within the Scope of this Policy.

❖ 3.5 Risk Assessment

Perform regular risk assessments on all information assets, and their supporting assets, as detailed within the SGT Risk Assessment and Risk Management Procedure, and using the control objectives and

controls as documented within Annex A of ISO/IEC27001:2017 and others selected by SGT as relevant to what they do. The documented results of risk assessments shall be reviewed to understand the level of risk to information and supporting assets, and appropriate controls implemented as appropriate to address any unacceptable risks that have been identified. A Statement of Applicability (SoA) shall be produced to record which controls have been selected and the reasons for their selection, and the justification for any controls not selected.

ISMS risks are presented to the SGT Risk Committee alongside the separately maintained Organisational risk register (this has a separate risk management methodology) and manages risks such as supplier failure.

- **3.5.1 Control of Supply Chain Risks**

SGT relies upon suppliers of products and services to perform its work. Suppliers are approved, monitored and managed according to the criticality of the item supplied, which can be briefly grouped into the following categories:

- Critical Data and Infrastructure services – these are contracted from a handful of suppliers. Any change (new supplier, alternate supplier etc.) will be reviewed and accepted by the ISMS Steering Committee (ISMS SC). Performance is reviewed at ISMS SC meetings. ISO 27001 compliance can be a key source of information to support such approvals. Products or service under this level of control include:
- Control or provisioning of network infrastructure or monitoring (including penetration testing and hosting bandwidth / connectivity suppliers)
- Data or information-carrying equipment storage or disposal (e.g. confidential shredding, off-site archiving etc.)
- Provision of software management services, licensing etc.
- Delivery services including Royal Mail
- Purchase of commodity IT equipment and software. These items are sourced from reputable suppliers, generally returned to a bare-metal or clean firmware state before use. The ICT supply chain is overseen by the Service Desk
- Low-criticality support products or services – these are services without a direct affect on Information Security Objectives, or where information security risks are already controlled without reliance on the behaviour or performance of the supplier.

The company financial control procedures are applied to the approval of any new supplier using the Supplier Information Security Questionnaire. This complements rather than replaces the controls above

❖ 3.6 Information Security Incidents

Provide a mechanism for the prompt identification, reporting, investigation and closure of information security incidents[5] to SGT, in accordance with the Incident Management Policy, and to fully analyse reported incidents to identify the root cause of issues and take advantage of any improvement opportunities which may have been identified.

[5] This includes 'exceptions' - condition that can arise during execution of a computer program, that can cause a deviation from the normal execution sequence, and for which means exist to handle it https://electropedia.org/iev/iev.nsf/display?openform&ievref=171-05-70

❖ 3.7 Access to Information and Systems

Ensure that an Access Control Policy is in place to protect all SGT networks, information systems and information assets from any unauthorised access. Legitimate remote access shall only be granted in accordance with the policy to bona-fide personnel, contractors and third party users, and only applies to access from SGT approved devices. Remote connections shall be used strictly in accordance with the Acceptable Use Policy. Remote access shall be regularly reviewed and any connections that are no longer required shall be removed immediately.

❖ 3.8 Business Continuity Management

Ensure that information security is a key consideration within the Business Continuity Management Plan, so that the security of SGT information assets is not compromised even when faced with a wide variety of unplanned business interruptions. The Business Continuity approach is based on undertaking a business impact analysis to determine what systems and services are critical to SGT, and ensuring they are put in place first.

❖ 3.9 Information Security Training

SGT will implement processes and procedures to enable staff to confidently hand and process data using the systems and network in place.

Perform regular Information Security training and education which shall be mandatory for all SGT employees, contractors and third party users.

- New employees, contractors or third party users shall be required to undertake initial information security training as soon as possible after joining SGT.
- On a periodic basis, and at least annually, SGT shall provide refresher information security training or updates, whichever is appropriate, which is mandatory for all personnel. This shall cover changes in SGT's approach to information security, changes to relevant information security processes and communicate any new or changing risks that SGT may be facing.
- SGT shall provide detailed training to those individuals who have specific roles and responsibilities in delivering the ISMS.
- Information security training shall be provided by any suitable means, including physical training, on-line presentations, educational documentation etc. Records of all training undertaken shall be maintained, and the effectiveness of different training formats reviewed.

Information security training shall address key items from the following:

- the ISMS Policy (this document)
- Information classifications as per the Classification and Handling Guide
- the Acceptable Use Policy and its requirements
- the use of passwords as per the Acceptable Use Policy
- how to ensure appropriate protection from virus and malware as per the Anti-Virus and Vulnerability Management Policy
- the identification and reporting of information security incidents as per the Incident Management Policy

- the Social Media Policy

❖ 3.10 Management, Monitoring and Review

Continually monitor, review and improve the SGT ISMS by undertaking regular reviews, internal audits (in accordance with the Internal Audit Policy) and other related activities, and taking prompt corrective actions and implementing improvement opportunities in response to the findings of these activities. This includes evaluation of requests for exemptions from the requirements of the ISMS – these requests will be made to the Data Protection Team and need to be authorised via email before they take force; if they are authorised it will be for an agreed time, an item will be added to the Corrective Action Log so they can be monitored.

There will be a monthly summary for the Senior Management Team (SMT) on incidents, issues, opportunities for improvements and changes that may have an impact on the effectiveness of the ISMS.

The ISMS SC will meet every six months, ad-hoc meetings can be called to deal with any urgent issues. The agenda will be:

- Actions from the last meeting
- Changes affecting the ISMS – internal, external, regulatory etc.
- Risk assessment and treatment, including updates and vulnerabilities or threats not adequately addressed in previous risk assessments
- Progress on objectives, opportunities for improvements, performance information (including results from effectiveness measurements and internal ISMS awareness) and feedback from interested parties
- Incidents
- Corrective actions
- Audit results (non-conformities and observations), progress on actions raised
- Updates to policies, guidelines, Statement of Applicability, asset registers, etc.

An Annual Review document will be produced and presented to the ISMS for discussion and planning of future work on the ISMS. This will include:

- a review of the risk assessments completed over the previous year
- agreement on a plan for risk assessments for the forthcoming year
- a review of any risk treatment activities over the previous year
- agreement on any residual/accepted risks being carried into the forthcoming year
- a review of internal audits and non-conformances raised over the previous year
- agreement on a plan for internal audits for the forthcoming year
- a review of information security incidents over the previous year
- a review of the previous year's information security objectives
- agreement on the information security objectives for the forthcoming year
- a review of the Information Security Policy
- a review of the ISMS Policy
- a review of the ongoing suitability of the ISMS to meet the requirements of ISO27001
- a review of the effectiveness of security training over the previous year
- a review of feedback from stakeholders/interested parties over the previous year
- a review of any planned business changes which may affect operation of the ISMS
- consideration of any suggestions for improving the overall operation of the ISMS

❖ 3.11 Legislative Compliance

Ensure that, at all times, its Information Security Management System shall support full compliance with the following UK legislation and regulations, including but not limited to:

- Data Protection Act 2018, UK GDPR and EU GDPR (see Appendix 2 for more details)
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988 (see Appendix 3 for more details)
- Companies Act 1985
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Waste Electrical and Electronic Equipment Directive (WEEE) 2003
- Malicious Communications Act 1988
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Contracts Act 1990
- The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA)
- Freedom of Information (Scotland) Act 2002
- The Defamation and Malicious Publication (Scotland) Act 2021
- Wales Accord on the Sharing of Personal Information (WASPI) 2018

SGT policy is to comply with any legally issued request from UK authorities mandating disclosure of data held. Any such request will be reviewed and confirmed by the Information Security Steering Committee. In extreme circumstances, a member of the Steering Committee shall authorise the urgent request and report this to the committee as soon as is practical. SGT is committed to disclosing this action to the organisation to whom the data relates (or the client the data is held on behalf of them) prior to any disclosure or as soon as legally permitted.

❖ 3.12 Document Management

ISMS Documents will carry a standard Document Control section setting out the documents history, revisions and approvals. The control section is optional for other documents; its use across SGT documents will be encouraged and supported by the ISMS SC.

The current version of all ISMS documents are available from the Information Security Manager for internal use and can be released to external parties in response to specific needs (i.e. to confirm the systems that SGT operate). Only the version supplied by the Information Security Manager is guaranteed to accurately reflect the latest approved version, hence required documents must be obtained from this source every time – printed copies must only be considered accurate at the point of printing.

All documents are approved by the ISMS SC prior to issue and reviewed on an annual basis or whenever changes to arrangements or activities occur. The ‘Monthly Timetable’ contains the master list of ISMS documents, owners, latest version id and review schedule.

4.0 ISMS RESPONSIBILITIES

❖ 4.1 Employees, Contractors and Third Party Users

Within SGT, all employees, contractors and third party users shall understand their role in ensuring the security of information assets (and their supporting assets) in accordance with the Information Security Training Policy as detailed in Section 3.9. Key personal responsibilities include:

- Acting as a responsible professional, respecting policies in place to take care of the information entrusted to them or to which they have access
- Being aware and informed about Information Security and the risks we face
- Reporting instances where the system falls short of our expectations as an Information Security Incident
- Identifying changes to the risks we face or where our controls appear to leave risks inadequately addressed
- Respecting rules and controls in place

SGT has opted against creating a large, central function to manage Information Security – everyone contributing in this way helps to ensure that the system reflects our values and needs as it delivers strong Information Security.

There are, however, additional responsibilities defined in order that the ISMS shall operate efficiently and in accordance with the requirements of ISO/IEC 27001:2017. These are detailed below.

❖ 4.2 Senior Management

The Chief Executive Officer and SMT shall be responsible for the following activities within the SGT ISMS:

- Agreeing the business need for this ISMS, and communicating their ongoing commitment to it
- Reviewing and signing off this Information Security Policy
- Setting and reviewing SGT's Information Security Objectives
- Assigning appropriate resources necessary to manage and operate the ISMS effectively
- Agreeing the level of acceptable risk within the Risk Assessment and Risk Management Procedure
- Approving any decisions not to address any unacceptable residual risks, where identified
- Having ultimate responsibility for actions related to information security incidents/breaches
- Overseeing any disciplinary action resulting from information security incidents/breaches
- Ensuring an effective 'whistleblowing' process is in place

❖ 4.3 Information Security Manager

The Information Security Manager shall have functional responsibility for the SGT ISMS, and shall be responsible for the daily operational tasks of the ISMS, including:

- Ensuring an appropriate structure of ISMS policies, processes and work instructions
- Ensuring that appropriate records are created and maintained for all ISMS activities
- Ensuring the ISMS operates in accordance with the current requirements of ISO27001:2017
- Arranging a programme of risk assessments, risk treatments and internal audits
- The preparation and communication of the Statement of Applicability

- Appropriate communication about the ISMS, including to third parties (see Appendix 4 Communications) and reporting on performance on the ISMS
- The provision of an appropriate user training and awareness programme for employees
- Overall management of the information security controls in business processes
- Overall management and functionality of SGT's business continuity plan
- The provision of a user training and awareness programme for suppliers and contractors
- Overall management of the design and review of technical security controls, including SGT networks, threat intelligence management (see Appendix 5 Threat Intelligence Management), contact with authorities (see Appendix 6 Contact with Authorities) and contact with special interest groups (see Appendix 7 Contact with Special Interest Groups)
- Supporting reviews, internal audits and risk assessments; reviews and audits to be done by independent parties where practicable
- Maintaining appropriate contacts with relevant authorities (including utilities and the emergency services) to support incident management, business continuity planning and anticipate and prepare for upcoming changes in laws or regulations

❖ 4.4 Managers

Managers within SGT shall be responsible for:

- Ensuring their team members are aware of and remain compliant with all information security policies, processes and work instructions, and that they receive appropriate training
- The provision of a user training and awareness programme for applicable third party users
- Supporting reviews, internal audits and risk assessments within their area of responsibility
- Transferring knowledge from leavers so there is continuity in providing services
- Ensuring segregation of duties on ISMS tasks where this is achievable and appropriate

❖ 4.5 Asset Owners

Asset Owners shall be responsible for:

- Assessing the value of their asset(s) to SGT
- Undertaking detailed risk assessments on their asset(s), including the identification of controls and assessing their effectiveness (as per the Risk Assessment and Risk Management Procedure)
- Addressing any significant risks (as per the Risk Assessment and Risk Management Procedure)
- Assisting in the investigation, resolution and closure of any information security incident which directly or indirectly affects the security of their asset(s)
- Reviewing and authorising the levels of access to their asset(s) which are granted to others (as per the Access Control Policy)
- Contributing to the Acceptable Use Policy, specifically for the use of their asset(s)

❖ 4.6 Control Owners

Control Owners shall be responsible for:

- The way in which their assigned control(s) are selected, implemented and operated
- Understanding which asset(s) are reliant upon each of their assigned controls
- Providing feedback to asset owners on the operation of each control, to assist them in undertaking accurate risk assessments of their asset(s)
- Assisting in the investigation, resolution and closure of any information security incident which actually or potentially indicates the failure of a control

5.0 DOCUMENT CONTROL

This Policy needs to be formally reviewed on a per annum basis, as a minimum, or if required changes are identified to address one or more of the following:

- A change in business activities, which will or could possibly affect the current operation of the SGT Information Security Management System.
- A change in the manner in which the SGT manages or operates its information assets and/or their supporting assets.
- An identified shortcoming in the effectiveness of this Policy, for example as a result of a reported information security incident or an audit finding.

The current version of this Policy, together with its previous versions, shall be recorded below.

Version	Description	
1.0	Date Live:	27 March 2017
	Version Notes:	First version
	Reviewed by:	Malcolm Walker, Assistant Chief Executive
	Approved by:	ISMS Steering Committee
1.1	Date Live:	20 July 2017
	Version Notes:	2.0 Policy Scope - Information stored in prisons, and the way work is done within prisons, is outside of the scope of this policy. 6.0 Appendix 1 – Interested parties a) added information about employees location b) added details of external users of HR systems Changed address of Ipswich Office Supply chain - overseen by the Service Desk, previously the ICT Manager Updated Owner to 'Assistant Chief Executive'
	Reviewed by:	Malcolm Walker, Assistant Chief Executive
	Approved by:	ISMS Steering Committee, 28 November 2017
1.2	Date Live:	05 March 2018
	Version Notes:	Changed address of Cardiff Office
	Reviewed by:	Malcolm Walker, Assistant Chief Executive
	Approved by:	ISMS Steering Committee, 20 March 2018
1.3	Date Live:	24 May 2018
	Version Notes:	Updated references of Data Protection Act 1998 to Data Protection Act 2018 Corrected typos and put details about Copyright into Appendix 3
	Reviewed by:	Malcolm Walker, Assistant Chief Executive
	Approved by:	ISMS Steering Committee
1.3.1	Date Live:	30 October 2018
	Version Notes:	Updated title to include Data Protection. Add (aka ISMS policy) to 2nd last bullet point on p1. Update section 4.1 reference to 3.9
	Reviewed by:	Malcolm Walker, Assistant Chief Executive
	Approved by:	ISMS Steering Committee
1.4	Date Live:	10 January 2019

	Version Notes:	Added 7.7 Meeting data protection requirements for children's data to provide details about the processing of children's data.
	Reviewed by:	Malcolm Walker, Assistant Chief Executive
	Approved by:	ISMS Steering Committee
1.5	Date Live:	22 February 2019
	Version Notes:	Added details to 7.6 Data protection by Design and Default on anonymization by encryption and pseudonymisation and the use of DPIAs when considering processing conducted wholly or partially by automated means
	Reviewed by:	Malcolm Walker, Assistant Chief Executive
	Approved by:	ISMS Steering Committee
1.6	Date Live:	26 July 2019
	Version Notes:	Updated first page to include reference to ISO27001 and Atlas Offices - added Wrexham, updated address of Leeds, indicated which offices are used on a part time basis Removed references to Concessions – they had never been used Various refences to Data Protection Requirements (3.1, 3.9, 7.2, 7.6-7.10, 7.12)
	Reviewed by:	Ian Grey (WADIFF Consulting)
	Approved by:	Malcolm Walker, Assistant Chief Executive
1.7	Date Live:	24 April 2020
	Version Notes:	Offices - added Coventry and Maidstone
	Reviewed by:	Malcolm Walker
	Approved by:	Malcolm Walker, Assistant Chief Executive
1.8	Date Live:	05 Nov 2020
	Version Notes:	Rebranded document and updated offices
	Reviewed by:	Malcolm Walker
	Approved by:	Steering Committee
1.9	Date Live:	07 April 2021
	Version Notes:	Changes to wording in 3.11 and 7.0 appendix 2 in relation to UK GDPR
	Reviewed by:	Malcolm Walker
	Approved by:	Steering Committee
2.0	Date Live:	05 Nov 2021
	Version Notes:	Updated section 2.0 scope to include Swansea, Newport & Wolverhampton offices
	Reviewed by:	Malcolm Walker
	Approved by:	Steering Committee
2.1		01 Nov 2022
		Updated section 2.0 scope to include Norwich office
		Malcolm Walker
		Steering Committee
3.0	Date Live:	22 March 2023
	Version Notes:	Added header to confirm this document is the Information Security policy

		Added summary at the start on purpose of the ISMS and what it covers Changed 'ISO27001:2013' to 'ISO27001:2017' Change text of the ISMS Scope Added footnote to confirm 'employees' includes volunteers Added 1.1 Organisation objectives for the ISMS so the objectives are explicitly stated, links objectives to the KPIs Updated section 2.0 scope – updated Norwich office location, added York office Updated 3.5 Risk Assessment– reference to Organisational Risk Register Update 4.2 Senior Management responsibilities Updated 4.3 Information Security Manager responsibilities Updated 4.4 Managers responsibilities Updated 3.6 Information Security Incidents – dealing with exceptions Updated 3.10 Management, Monitoring and Review – dealing with exemptions Updated 3.11 Legislative Compliance – added • The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) • Freedom of Information (Scotland) Act 2002 • The Defamation and Malicious Publication (Scotland) Act 2021 • Wales Accord on the Sharing of Personal Information (WASPI) 2018 Updated 3.12 Document Management, reference to 'Monthly Timetable' containing the master list of ISMS documents, owners, latest version id and review schedule Updated Appendix 1 Interested parties – added more details about expectations of each party Added Appendix 4 Communications Added Appendix 5 Threat Intelligence Management Added Appendix 6 Contact with Authorities Added Appendix 7 Contact with Special Interest Groups Some of these updates made to prepare for ISO27001:2022
	Reviewed by:	Malcolm Walker
	Approved by:	Steering Committee

6.0 APPENDIX 1 – INTERESTED PARTIES

The key interested parties and their main information security requirements are:

Interested party	Expectations
Clients	Clients expect confidentiality when SGT process their personal data and have that it is available and accurate when they interact with SGT. They expect SGT and its systems to support compliance with Data Protection legislation.
Employees (full time, part time, volunteers and contractors) working in SGT offices and remotely	Those working for and with SGT can expect that their details and details of their relationship with SGT are treated confidentially and maintained with sufficient integrity and availability to efficiently manage this relationship. They also expect Clear Review to comply with its economic and contractual obligations to them and provide safe working conditions. They can expect appropriate training and support from SGT Review to help them understand and discharge the information security implications of their role. **NOTE**: anyone working within a prison will follow the security requirements of the Prison service while they are there
External users of HR systems for recording holidays etc.	Users of HR systems expect that their details and details of their relationship with SGT are treated confidentially and maintained with sufficient integrity and availability to efficiently manage this relationship.
Trustees	Trustees expect that their details are treated confidentially and maintained with sufficient integrity and availability to efficiently manage this relationship in a way that allows them to meet legal obligations for being a Trustee.
Donors	Donors expect that their details are treated confidentially and maintained with sufficient integrity and availability to efficiently manage this relationship.
Partner Agencies	Partner agencies expect details shared with SGT are treated with an appropriate level of confidentially, integrity and availability to efficiently manage this relationship and meet legal obligations
Government Bodies, incudes Funders	Government bodies expect that details shared with SGT are treated with an appropriate level of confidentially, integrity and availability to efficiently manage this relationship and meet legal obligations
Suppliers (the supply chain)	Suppliers can expect that their details and contractual relationship with SGT are treated confidentially and maintained with sufficient integrity and availability to efficiently manage this relationship. They also expect Clear Review to comply with its economic and contractual obligations to them
Regulators	The Information Commissioners Office expect SGT to meet legal obligations in the way it processes personal information. The Charity Commission expects that details shared with SGT are treated with an appropriate level of confidentially and maintained with sufficient integrity and availability to efficiently manage this relationship and meet legal obligations

7.0 APPENDIX 2 – DATA PROTECTION ACT

The Data Protection Act 2018 (referred to as the DPA from this point) regulates the use of personal information (information about an individual, rather than an organisation) whether in hard copy or electronic format. The DPA applies the UK GDPR (General Data Protection Regulation), the EU GDPR can also be relevant for SGT if there are personal details of people in the EU, e.g. collected by Fundraising.

The Data Protection (Charges and Information) Regulations 2018 requires organisations handling, storing or processing personal data that is not covered by a specific exemption to register with the Information Commissioner's Office and pay an annual fee. SGT has nominated to register the Assistant Chief Executive as the main point of contact to ensure compliance as activities evolve and to provide reassurance to members of the public who wish to know more about how SGT handle data.

❖ 7.1 Data Protection Definitions (from Articles 4 and 9 of the GDPR)

Personal Data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". This is a wide ranging definition and the use of "directly or indirectly" means that information that on its own may not be able to identify an individual, e.g. a post code, may be able to identify them if combined with other data.

Sensitive/Special Data means "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

Data Controller means "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". This is SGT when determining the use of personal data including donors and staff.

Data Processor means "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". This is SGT when undertaking work on behalf of other bodies, including partners. The contract with SGT will identify that it is acting as a Controller and define data protection requirements.

Processing means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

Personal Data Breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise

processed". This is different to a Personal Data Loss where personal data has been obtained by an unauthorised third party. Backup failures or seeing personal data on a screen would be breaches. The Incident Management policy defines the steps to be taken if there has been a personal data breach, for example, informing the Information Commissioner's Office within 72 hours of becoming aware of it if the breach is likely to present a risk to people's rights and freedoms.

❖ 7.2 Data Protection Principles

There are six data protection principles that are central to the DPA, these are taken from the GDPR. In brief, the principles are:

- Processed lawfully, fairly and in a transparent manner. There are six lawful ways to process data
  - ***Consent*** - Personal data may be processed on the basis that the data subject has consented to such processing.
  - ***Contractual necessity*** - Personal data may be processed on the basis that such processing is necessary in order to enter into or perform a contract with the data subject.
  - ***Compliance with legal obligations*** - Personal data may be processed on the basis that the controller has a legal obligation to perform such processing.
  - ***Vital interests*** - Personal data may be processed on the basis that it is necessary to protect the "vital interests" of the data subject (this essentially applies in "life or-death" scenarios).
  - ***Public interest*** - Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.
  - ***Legitimate interests*** - Personal data may be processed on the basis that the controller has a legitimate interest in processing those data, provided that such legitimate interest is not overridden by the rights or freedoms of the affected data subjects.
- Purpose limitation - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Data minimisation - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accuracy - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Storage limitation - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The Retention policy defines how long different types of personal data need to be kept.
- integrity and confidentiality - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. There are a robust set of internal controls and procedures to monitor access to systems, and levels of system access are subject to regular audits. Access to our systems is by unique login, use of strong passwords is required. The sharing of logins and passwords I strictly prohibited and may render employee(s) liable to disciplinary action.

There is a seventh principle – Accountability – for the Data Controller to demonstrate compliance with the other principles. The ISO27001 internal audits programme is the main way the check that this principle is met.

❖ 7.2 Rights of Individuals

SGT recognises the legal rights of those whose data it is processing or intends to process and will ensure that appropriate information is provided to them advising them of their rights, and that policies and procedures are maintained to ensure that SGT is able to recognise information rights requests and handle them appropriately when they are exercised. In brief, the rights are:

- The right to be informed – providing information about how personal data will be processed and the rights of individuals at the point where personal data is collected
- The right of access ('Subject Access Request') – allow individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing. Third party details may need to be redacted
- The right to rectification – to have personal data updated it is inaccurate or incomplete
- The right to erasure (the 'right to be forgotten') – allow individuals to request the deletion or removal of personal data where there is no compelling reason for its continued processing. If there is a reason, the personal data does not have to be deleted
- The right to restrict processing – allow individuals to 'block' or suppress processing of their personal data when one of the following apply:
    - the accuracy of the personal data is contested by the individual, for a period enabling the controller to verify the accuracy of the personal data
    - the processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of their use instead
    - the controller no longer needs the personal data for the purposes of the processing, but they are required by the individual for the establishment, exercise or defence of legal claims
    - the individual has objected to processing (the Right to Object) and wants processing halted under this is resolved
- The right to data portability – allows individuals to get a copy of their personal data. Applies where processing is based on consent ***or*** a contract and is carried out by automated means (manual/paper systems are excluded). Data needs to be exported in a commonly used and machine readable format, e.g. CSV or PDF
- The right to object – allows individuals to stop the processing of personal data. Applies where processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- Rights in relation to automated decision making and profiling – allows individuals to access to information about the reasoning behind any decisions taken by automated means

❖ 7.3 Employee data

SGT needs to collect and use certain types of information about employees, including the information contained in the employee's confidential personnel file, in order to operate and fulfil legal obligations.

SGT will hold such information only for as long as we consider necessary to fulfil the purpose for which it was obtained, and process it (including disposing and destroying it) in accordance with the Data Protection Principles and other requirements of the DPA and any other procedures laid down by SGT for this purpose from time to time. The Retention Policy defines how long different types of personal data will be retained. The ISMS defines retention periods for records that demonstrate individual competence and adherence to the systems principles well beyond their employment to allow for audit and improvement of the management system.

SGT will take all reasonable precautions to ensure that, to the best of our knowledge and belief, the details contained in the employee's personnel file are correct and, at all times, to guard information against any unauthorised access and use.

Every employee of SGT has a responsibility not to use or pass on another employee's personal information (including, but not limited to, home contact details, birthday date and photographs) without the express written consent of the individual to whom the personal data relates.

❖ 7.4 Client and Partner Employee Data

In the course of the work we do, we are given access to the personal details of clients and for employees of our partners (e.g. contact or biographical details to identify an authorised user). This personal information is confidential and must be protected and processed in accordance with the DPA. It must not be passed on to third parties, taken off site in any format, or processed in any way without the express written consent of the client and/or the client's employee. These objectives are achieved by the Secret classification applied to such information.

❖ 7.5 Analytics, Log and Usage Data

Data itemising and analysing usage of our web sites is collected to provide valuable business intelligence. It is a core principle that no attempt will be made to link uniquely identified visitors with personal identifiable information. Likewise, such data will not be used to discriminate against individuals or vary the level of service they receive. These principles are vital to ensuring that this data is used for legitimate analytics purposes and does not become personal information as defined by the act.

CCTV Images and Video

Given that CCTV surveillance is used within SGT premises, captured images and video (either through routine recording of the CCTV feed or an authorised user's decision to capture a particular event), will constitute personal information of any individuals captured as defined by the act. CCTV is used exclusively in areas where no individual would have a reasonable expectation to privacy and with clear signage to indicate its use and provide further contact details.

Compliance Procedures

Where Personal Data is handled by SGT, it will be afforded protection at Secret level as per the information classification scheme.

SGT employees who handle personal information for specific projects will be required to sign our Compliance Register to acknowledge their understanding of the DPA and their responsibilities as data handlers.

Where Personal Information is handled on behalf of the company itself, this will be as a core function of the individual's role (e.g. HR access to employee personal data) or by senior management. This allocation of responsibilities ensures that DPA obligations are fully understood, reinforced contractually and responsibly adhered to.

Failure to comply with the DPA by any employee of SGT will be investigated. If it is found that an employee has deliberately failed to comply with the DPA, or has wilfully misused personal information, he or she will be subject to the SGT's disciplinary procedure.

Any employee of SGT who thinks that a colleague may be misusing personal information or breaching the terms of the DPA must report the matter as an Information Security Incident.

❖ 7.6 Consent

Consent shall not be valid unless:

- There is a genuine choice
- It has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subjects wishes that signifies agreement to the processing of personal data relating to them
- The consent was given through statement made by the data subject or by a clear affirmative action undertaken by them
- SGT can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully
- A mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent in effect as easy as it was to give, and the data subject has been informed about how to exercise their right to withdraw consent.

SGT recognises that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject. SGT recognises that consent cannot be considered to be forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing.

❖ 7.7 Data Processors

When acting as a Data Controller - SGT reserves the right to contract out data processing activities or operations involving the processing of personal data in the interest of business efficiency and effectiveness. No third-party data processors will be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation. Colleagues wishing to appoint a data processor will ensure that appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment. The DPO will provide advice and guidance in respect of this. A written agreement will be implemented between the SGT and the data processor which meets the requirements of the Data Protection Legislation. The DPO will ensure that a register of such agreements/arrangements is maintained. The data processor agreement will specify what is to happen to personal data upon termination of the data processing agreement.

When acting as a Data Processor - SGT will get written permission form the Data Controller before appointing any sub processor.

No employee is permitted to commission or appoint a third party to process data on behalf of SGT without adhering to this policy.

❖ 7.8 Data sharing, disclosure and transfer

When acting as a Data Controller - SGT will only share personal data with or otherwise disclose personal data to third parties where there is a legal basis for doing so and the data sharing is necessary for the specified purposes. No data sharing or disclosure is permitted to occur without a suitable legally enforceable agreement satisfying the requirements for such agreements as set out in the Data Protection Legislation. Data sharing agreements must be approved by the DPO who will maintain the register of all such agreements. Appropriate risk assessments will be undertaken prior to any data sharing taking place on those with whom we intend to share personal data.

When acting as a Data Processor - SGT will only share personal data where this is is part of contractual arrangements, and to the names parties in the contract.

SGT will provide information to all employees setting out safe and approved methods of transferring personal data to recipients. Employees are required to use only approved methods of data transfers. Disciplinary action will be taken against employees who fail to observe the data transfer policy and use unsafe and insecure methods of data transfer unless such methods have been approved in writing by the DPO.

❖ 7.9 International Transfers

When acting as a Data Controller - SGT will neither transfer nor process not will it permit personal data to be transferred or processed outside the United Kingdom without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that the SGT undertakes or commissions whether directly or indirectly must be approved by the DPO and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK's Information Commissioner;
    - The territory into which the data are being transferred is within the European Economic Area;
    - The territory into which the data are being transferred has an adequacy decision issued by the European Commission;
    - The transfer is to the United States of America and the recipient is registered under the EU/US Privacy Shield scheme;
    - The transfer is made under the unaltered terms of the standard contractual clauses issued by the European Commission for such purposes;
    - The transfer is made under the provision of binding corporate rules which have been approved and certified by the European Commission;
    - The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

When acting as a Data Processor - SGT will only transfer personal data to location/parties specified in the contract.

❖ 7.10 Data protection by Design and Default

There is an obligation to implement appropriate technical and organisational measures to consider data protection issues at all times. SGT achieve this by actions such as:

- performing Data Protection Impact Assessments (DPIA) and when using new technologies/introducing new systems and processes, and processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA needs to be done when processing is 'conducted wholly or partially by automated means'. For SGT it is likely to cover some fundraising activities including sending emails to subsets of donors, and potentially the use of cookies on the SGT website Actions coming out of DPIAs can include anonymization by encryption and/or pseudonymisation and allowing individuals to monitor the processing being done on them
- ensuring no action is required on the part of the individual to protect their privacy – it is built in and enabled by default
- creating and improving security features on an ongoing basis

Encryption is a mathematical function using a secret value—the key—which encodes data so that only users with access to that key can read the information. It is part of HTTPS secure connections and can be used to secure data 'at rest' on desktops, laptops, USB devices etc.

Pseudonymisation is the process of changing data so individuals are referenced by an identifier rather than their 'real world' identity.

Details of using encryption and pseudonymisation can be found on the ICO website.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/

https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

❖ 7.11 Meeting data protection requirements for children's data

Data on children may need to be collected and processed to provide our services. This could be directly to the child or indirectly to provide services to their parent or guardian. The age of a child is defined in the DPA2018 as up to 13 (Part 2, Chapter 2(9)). SGT consider anyone under 18 as a child; this is defined in the Safeguarding Children Policy. Anyone working with children will be DBS checked (part of standard HR procedures). The Safeguarding lead is Maria McNicholl and there is a Safeguarding panel; see the Safeguarding Clients at Risk Policy for details of who is on the panel.

Personal data is processed on the basis of consent. A Confidentiality and Information Sharing Agreement needs to be completed before services can be provided. This provides details on the confidentiality of information, the rights of the individual over their data and how they can be exercised, how they can withdraw their consent and allows the individual to define who we can contact to get more information and where we can share their details. The text on the agreement aims to avoid complicated language to it can be easily understood.

❖ 7.12 Personal Data Breaches

All employees and individuals with access to personal data for which SGT is either data controller or processor must report all personal breaches to an appropriate individual as set out in the Incident Management Policy as soon as they become aware of the breach. SGT will log all personal data breaches and will investigate each incident without delay.

8.0 APPENDIX 3 – SOFTWARE COPYRIGHT AND INTELLECTUAL PROPERTY

Software Copyright

The Copyright, Designs and Patents Act 1988 states: The owner of the copyright has the exclusive right to copy the work (Section 16). That means it is illegal to copy software without the copyright owner's permission. With regard to software, the copyright owner is the software developer / publisher, and use of software without (or outside the terms of) a license to do so from them will not be tolerated.

SGT is committed to full compliance with Software Copyright through:

- Including installed commercial software and purchased licenses within the Asset Register to allow for robust assurance and audit that all software used has been correctly licensed
- Reviewing license terms and restrictions on 'free', community or open source software or services to ensure that these encompass the required scope of use and introducing any controls applicable to prevent exceeding any restrictions or limitations in place
- Embedding these controls within our Acceptable Use Policy and supporting policy documents, such that they can be applied to all systems under our control or used to work on our behalf.

Intellectual Property

SGT strongly believes in the value contained within the IPR of others. All SGT personnel are required to:

- Only use images or video where a suitable license has been purchased or granted
- Respect, protect and/or clearly identify intellectual property supplied by others

9.0 APPENDIX 4 – ISMS COMUNICATIONS

The ISO27001 standard requires communication about the purpose of the ISMS and how it works, including to interested parties. In SGT, this is part of communications to discuss issues relevant to the ISMS - including improvements to take advantage of new technologies and processes and to meet new contractual, legal and regulatory requirements - and determine actions required to keep the ISMS effective.

The scope of the communications is covering the ISMS framework and requirements of the selected controls, this includes policies and procedures and what individuals need to do.

What	When	With Whom	Who	How/Process
Purpose of the ISMS and what individuals need to do	Induction	Employees, Volunteers	Information Security Manager/ Data Protection team	Training session
Reminders about ISMS responsibilities, key results from audit and issues (where appropriate)	At least every 12 months	Employees, Volunteers	Information Security Manage/ Data Protection team	Updates at team meetings, organisation wide communications (usually emails)
Reminders to consider ISMS requirements, including data protection requirements such as use of secure emails	At start of projects	Employees, Volunteers	Managers or Team Leaders	Project kick off meetings
Updates on ISMS issues; changes to risks, summary of audit results, issues, opportunities for improvement and performance (KPIs)	Every 6 months	Senior Management team, Trustees	Information Security Manager	Verbally – supported by summary document, may be followed up with emails
Updates on ISMS issues; changes to risks, summary of audit results, issues, opportunities for improvement and performance (KPIs)	Every 6-9 months	Risk Committee	Information Security Manager	Verbally – supported by summary document, may be followed up with emails Some details from the Risk

What	When	With Whom	Who	How/Process
				Committee may feed back into the ISMS, e.g. adjusting the risk register
Purpose of the ISMS, providing sample documents (when requested)	Bidding for work	Potential funders	Managers or Team Leaders Data Protection team	Email or as part of contract schedule
Updates to key ISMS documents	As required and when updates are meaningful	Funders	Managers or Team Leaders Data Protection team	Email
Discuss changes relevant to the ISMS	Monthly	Central Services team heads	Information Security Manager/ Data Protection team	MS Teams call
IT Service Desk updates	Weekly	KCS May also include members of the Service Desk Data Protection team on first call of every month	Information Security Manager	MS Teams call Meting notes and relevant IT related status reports

Note: the review of ISMS documents by potential funders/funders, and replying to their questions about the ISMS, provides a level of independent checks to the effectiveness of the ISMS. Any issues raised will be fed back to the ISMS Steering Committee for evaluation

10.0 APPENDIX 5 – THREAT INTELLIGENCE MANAGEMENT

The St Giles Service Desk team meet at 9.30 am every Tuesday. The team have a key objective to ensure all members of the team are updated on all security, threat intelligence and vulnerabilities through this meeting. This information is obtained by the team and KCS from the National Cyber Security Centre (NCSC), key vendors such as Microsoft, VMware, Cisco and Citrix, and is consolidated into a weekly report which is minuted. In addition, SGT use N-Able to report on security issues identified by the N-Able system proactively, which includes real time monitoring of antivirus and anti malware scanning and protection status.

Issues raised and threat intelligence obtained is then discussed with the full service desk team to identify any actions that would be applicable to the technology stack, which are evaluated based on the security criticality and whether this is of relevance. Where actions are required, this is raised as a service desk ticket, with appropriate priority assigned based on the severity of the security or vulnerability issue identified. In the event there is an urgent vulnerability to address a service desk case would be raised for immediate action by the service desk team.

Threat intelligence may be shared with other organisations SGT works with if anything is identified that could have an impact on information shared with or between the organisations. Sharing would be done by the Data Protection Team.

The approach is defined through the implementation of the six key controls, namely:

1. establishing objectives for threat intelligence production through the service desk weekly forum and as approved by the data protection team in accordance with ISO 27001 objectives, as well as at management review where required to aid strategic cyber threat intelligence
2. identifying, vetting and selecting internal and external information sources that are necessary and appropriate to provide information required for the production of threat intelligence undertaken by reviewing the National Cyber Security Centre (NCSC) both as a source of threat intelligence as in order to identify and signpost additional external information sources as part of our operational cyber threat intelligence
3. collecting information from selected sources which is recorded in the weekly minutes of the meetings as part of our operational cyber threat intelligence
4. processing information collected to prepare it for analysis undertaken by the service desk team and presented to the meeting as part of our operational cyber threat intelligence
5. analysing information to understand how it relates and is meaningful to the organization during the meeting taking in to consideration technologies in the stack, risks and vendors as part of our tactical cyber threat intelligence
6. communicating and sharing it to relevant individuals in a format that can be understood through the minutes of the meetings and wider inclusion of the data protection team and management team as needed as part of the overall cyber threat intelligence approach

11.0 APPENDIX 6 – CONTACT WITH AUTHORITIES

Authority	How to contact/get updates	Responsibility
Charity Commission	https://www.gov.uk/government/organisations/charity-commission	Assistant CEO
Emergency Services	Dial 999 for Emergency Dial 101 for Non-Emergency Website for police force and fire service relevant for each office has contact details for general updates	Support Services
Utilities – water, electric, gas, ISP	Website for each utility has contact details	Support Services
National Cyber Crime Agency	https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime	Data Protection Team
National Cyber Security Centre	https://www.ncsc.gov.uk	KCS
Information Commissioners Office	Report a data breach https://ico.org.uk/for-organisations/report-a-breach/ Renew Data protection fee https://ico.org.uk/for-organisations/data-protection-fee/	Data Protection Team Data Protection Team
Insurers	Travelers Insurance Company Limited Tel: 0800 587 8388 https://www.travelers.co.uk/claims-centre	Support Services

12.0 APPENDIX 7 – CONTACT WITH SPECIAL INTEREST GROUPS

Special Interest Group	How to contact/get updates	Responsibility
Microsoft	https://technet.microsoft.com/security/advisory	KCS
VMware	https://www.vmware.com/security/advisories.html	KCS
Cisco	https://sec.cloudapps.cisco.com/security/center/publicationListing.x	KCS
Citrix	https://www.citrix.com/support/	KCS
Sonicwall	https://www.sonicwall.com/support/	KCS
MaaS360	https://www.ibm.com/docs/en/maas360	Support Services
Information Commissioners Office	https://ico.org.uk/	Data Protection Team
Data Protection People – data protection	Data Protection People are SGTs Data Protection Officer. https://dataprotectionpeople.com/ Contact using standard email and phone number – held by Data Protection Team	Data Protection Team
Bird & Bird – data protection	https://www.twobirds.com/en/capabilities/practices/privacy-and-data-protection/uk-and-eu-data-protection-bulletin	Data Protection Team