

INFORMATION GOVERNANCE

**EU- GENERAL DATA PROTECTION
REGULATION (May 2018)**

Audit Committee July 2017

WWW.SOMERSET.GOV.UK



Information Governance in SCC

Data Protection

Information Security – in partnership with ICT

Information Sharing

Records Management

Team of 6 employees

WWW.SOMERSET.GOV.UK



EU- GDPR – the Law

On May 25th 2018 the Data Protection Act 1998 will be repealed and the EU-General Data Protection Regulation (GDPR) will become law.

Assuming the Great Repeal Act comes into force the EU-GDPR will be adopted in UK legislation.


When the UK leaves the EU the GDPR or something very similar will be in place to provide “adequacy” and allow the UK to continue trading relations with the EU.

WWW.SOMERSET.GOV.UK



ICO Guidelines for compliance

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now



- 1 Awareness**

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.
- 2 Information you hold**

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.
- 3 Communicating privacy information**

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.
- 4 Individuals' rights**

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
- 5 Subject access requests**

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.
- 6 Lawful basis for processing personal data**

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.
- 7 Consent**

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.
- 8 Children**

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.
- 9 Data breaches**

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
- 10 Data Protection by Design and Data Protection Impact Assessments**

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.
- 11 Data Protection Officers**

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.
- 12 International**

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico. Information Commissioner's Office ico.org.uk

12/0 2017/01

WWW.SOMERSET.GOV.UK



Key Elements of EU-GDPR

1. Ensure Corporate Awareness
2. Know what personal data we hold
3. Communicate with data subjects (public / employees)
4. Uphold Data Subject Rights
5. Process Data Subject Access Requests (DSARs) on time
6. Ensure lawful basis for processing
7. Ensure consent is lawfully managed
 - Consider carefully if children are involved
8. Ensure contracts with processors are in place
9. Report and manage breaches effectively
10. Data Protection by design and default
11. Appoint a Data Protection Officer (DPO)
12. Ensure International transfers are lawful

WWW.SOMERSET.GOV.UK



ORG 00032 - Review

Risk Description: Information Governance: An event occurs that results in a statutory breach of data protection legislation. This could be an ICT security vulnerability that compromises the PSN network, a significant disclosure of sensitive personal data or another procedural breach of the EU GDPR.

Causes: An intentional exploitation of a security vulnerability in the SCC network by hostile agents such as hackers or malware.

A significant unintentional data breach of sensitive personal or business data in email, post, fax by an employee, contractor, service provider or an SCC Councillor.

Any non-compliance with the articles and recitals in the EU GDPR following implementation in May 2018.

Consequences: The Council is exposed to fraud, loss of reputation, legal action by clients or employees and / or the possibility of fines from the Information Commissioner's Office (currently estimated at £100k - £200k but potentially much higher in 2018).

Members of the Public are exposed to harm or distress due to the significant unauthorised disclosure of personal data.

WWW.SOMERSET.GOV.UK



SWAP Audits – IG programme

Last year as a preparation for GDPR Information Governance commissioned a series of audits from South West Audit Partnership (SWAP) which are now being completed.

- Information Sharing – completed
- GDPR Preparation – final draft
- Regulation of Investigatory Powers Act (RIPA)
 - Surveillance – final draft
- DSAR Processing – final draft

These audits will be being reported back by SWAP in due course

WWW.SOMERSET.GOV.UK



Priority 4 - SWAP recommendations

- **Information Sharing (completed)**
 - Better IG in smaller procurement contracts
 - Project Manager in IG for GDPR – Asset Register
- **GDPR preparations (final draft)**
 - Need to increase IG resources (WTE's)
 - Increase awareness in SCC
 - DPO to write a GDPR project brief
 - Appoint a GDPR Project Manager
- **RIPA (final draft)**
 - Review RIPA policy in respect of Social Media
- **DSARs (final draft)**
 - Implementation of a single system to monitor DSARs

WWW.SOMERSET.GOV.UK



Consequences of non-compliance 1

1. Financial Penalties

Potentially fines for non-compliance have been increased from £500,000 to a potential 20 million Euros / 4% of turnover.

However, it is unlikely that the UK Govt will impose fines that will financially cripple a public authority such as an NHS Trust or a Local Authority.

Fines for UK public bodies are likely to remain on a similar scale as they are now around £250,000.

WWW.SOMERSET.GOV.UK



Consequences of non-compliance 2

2. Loss or theft of personal data

Loss or theft of personal data from clients or employees could result in harm and or distress to the individuals affected. SCC currently holds very sensitive Social Care information and also data from partners such as the NHS and the Police.

3. Reputational Damage

If SCC were to have a significant breach of GDPR our reputation would be damaged with the public and our partners and trust in our organisation would be diminished.

WWW.SOMERSET.GOV.UK



Risks and mitigations 1

1. Corporate Awareness
 - Leadership buy in – SLT & Councillors
 - Employee training – Induction & Refresher
2. Know what personal data we hold, process and share
 - Data Audit – Information Asset Register
 - Information flow mapping
3. Communicate with data subjects (public / employees)
 - Public Privacy Notice (Your Somerset, website etc)
 - Employee contract notification
4. Uphold Data Subject Rights
 - Clear Notification
 - Processes in place

WWW.SOMERSET.GOV.UK



Risks and mitigations 2

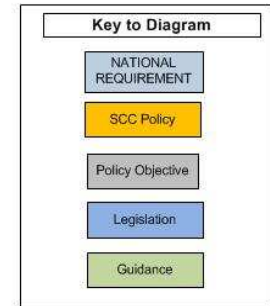
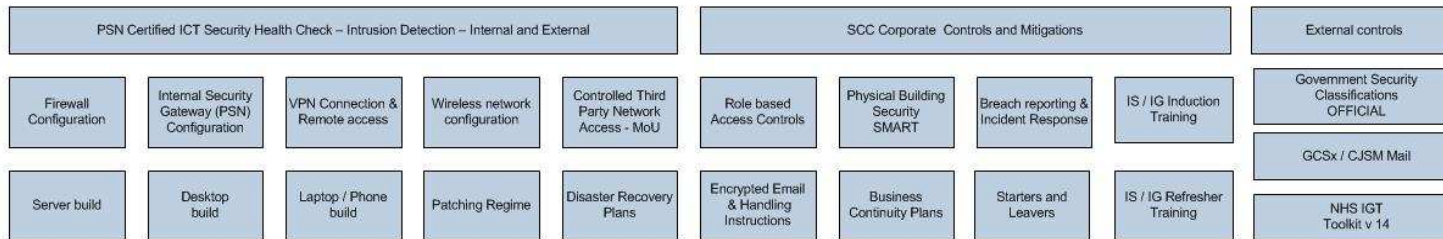
5. Process Data Subject Access Requests promptly
 - Adequate resources funded and in place
6. Ensure lawful basis for processing
 - Quality IG and legal advice
7. Ensure consent is lawfully managed
 - Good documentation
 - Employee training
8. Ensure contracts with processors are in place
 - Review and update employee contracts
 - Review and update processor contracts

Risk and Mitigations 3

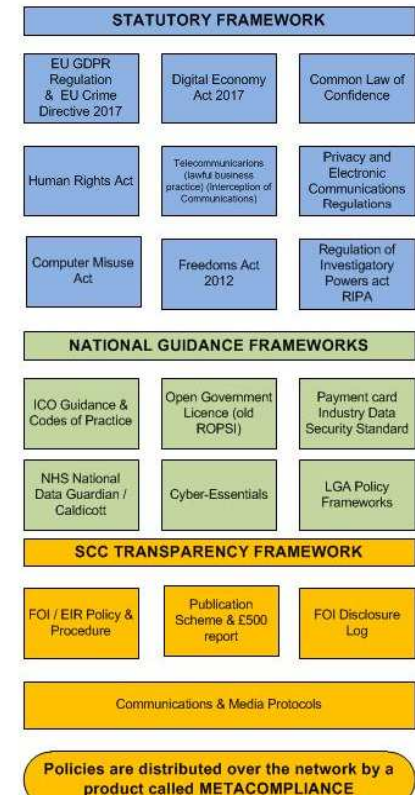
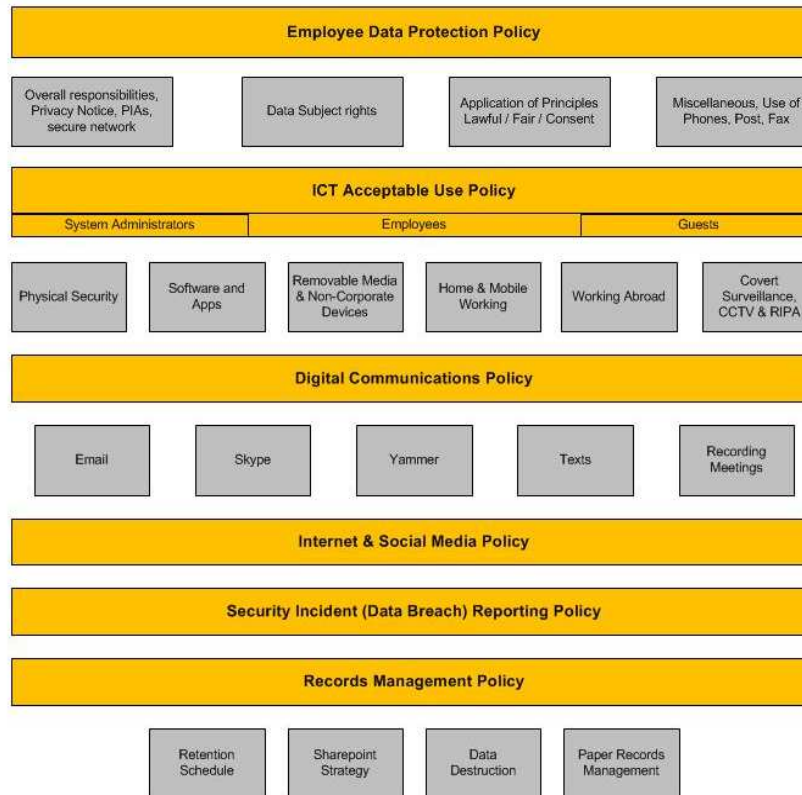
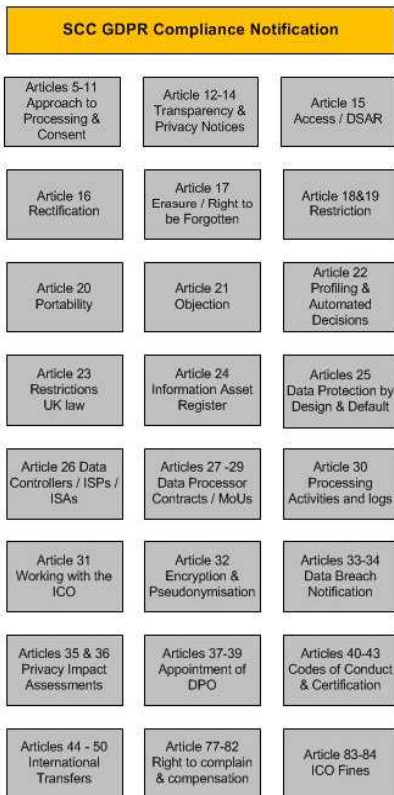
9. Report and manage breaches effectively
 - Update breach reporting procedure (72 hours)
10. Data Protection by design and default
 - Corporate awareness and training
 - Embed Privacy Impact assessments into projects
11. Appoint a Data Protection Officer (DPO)
 - IG Manager - Peter Grogan appointed as DPO
 - Ensure DPO is suitably resourced
12. Ensure International transfers are lawful
 - Good legal advice

INFORMATION GOVERNANCE – POLICY and GUIDANCE FRAMEWORK

PSN : N3 : Government : ICO and NHS IG Toolkit requirements



SCC CORPORATE INFORMATION SECURITY POLICY



Policies are distributed over the network by a product called METACOMPLIANCE

Personal commitment Statement included in Induction and Refresher training - (accepted / signed)

EU-GDPR implementation – Plan on a page

| ID | Task Name | Start | Finish | % Complete | 2017 | | | | | | | | | | | | 2018 | | | | | | | | | | | |
|----|---------------------------------|------------|------------|------------|---|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|--|-----|-----|-----|-----|-----|-----|-----|--|--|--|--|
| | | | | | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | | | | |
| 1 | Ensure Corporate Awareness | 01/05/2017 | 29/05/2018 | 15% | [Progress bar: 15% complete by May 2017] | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Know what personal data we hold | 03/04/2017 | 02/03/2018 | 10% | [Progress bar: 10% complete by April 2017] | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Communication | 01/05/2017 | 30/03/2018 | 5% | [Progress bar: 5% complete by May 2017] | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Data Subject Rights | 01/09/2017 | 01/06/2018 | 0% | | | | | | | | | | | | | [Progress bar: 0% complete] | | | | | | | | | | | |
| 5 | DSARs | 01/09/2017 | 31/05/2018 | 10% | | | | | | | | | | | | | [Progress bar: 10% complete by September 2017] | | | | | | | | | | | |
| 6 | Lawful basis | 03/04/2017 | 30/03/2018 | 10% | [Progress bar: 10% complete by April 2017] | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | Consent | 03/10/2017 | 03/09/2018 | 0% | | | | | | | | | | | | | [Progress bar: 0% complete] | | | | | | | | | | | |
| 8 | Contracts | 03/04/2017 | 03/07/2018 | 20% | [Progress bar: 20% complete by April 2017] | | | | | | | | | | | | | | | | | | | | | | | |
| 9 | Breach management | 03/08/2017 | 03/08/2018 | 0% | | | | | | | | | | | | | [Progress bar: 0% complete] | | | | | | | | | | | |
| 10 | Design & Default | 03/08/2017 | 03/08/2018 | 0% | | | | | | | | | | | | | [Progress bar: 0% complete] | | | | | | | | | | | |
| 11 | Appoint DPO | 03/04/2017 | 03/05/2017 | 100% | [Progress bar: 100% complete by April 2017] | | | | | | | | | | | | | | | | | | | | | | | |
| 12 | International transfers | 04/12/2017 | 03/08/2018 | 0% | | | | | | | | | | | | | [Progress bar: 0% complete] | | | | | | | | | | | |

WWW.SOMERSET.GOV.UK



Contacts

Peter Grogan, Information Governance Manager / DPO

07973 685784

PTGrogan@somerset.gov.uk

<http://enterprise.somerset.gov.uk/somerset/resources/clientservices/informationgovernance/>

WWW.SOMERSET.GOV.UK

