Information Security Policy

Document Owner	Data Protection Officer Tel: 03000 416814 Benjamin.Watts@kent.gov.uk
Version	V.5 December 2019
Approved	
Review	December 2020

Contents

Busy readers' summary

Citizens trust us with their personal information. Breaches or losses directly damage that trust and can put people at risk.

What are we protecting?

We must protect all personal information, especially information that may be sensitive or confidential, and business information that may be commercially or politically sensitive.

What level of security is required?

Kent County Council applies a risk-management approach to ensure security measures are proportionate and appropriate. The strength of a security measure therefore depends on the sensitivity of the information, its value to the business and the damage that might result from its unavailability, improper use, accidental disclosure, loss or destruction. The GDPR has brought a significant increase in the potential fines for data breaches of up to 20 million Euros. This has substantially increased the risk to KCC.

What kinds of security measures?

Security measures are broadly organisational measures (such as policies, management and training) which are supported and may be enforced by ICT security controls. KCC's ICT security is scrutinised by the Cabinet Officer for compliance with its Public Services Network Code of Connection and by the NHS for compliance with its Data Security and Protection Toolkit.

What must managers do?

Managers are responsible for security measures in their service areas and for ensuring policies are followed. They are expected to read and understand their information security responsibilities[1] and must ensure all employees complete mandatory data protection and information governance training. Managers must prioritise data privacy and embed in their operations the highest standards of information security. Records must be kept of all training as mitigation in the event of a breach.

Contract managers must assure contractor information security. KCC's standard contracts and service agreements include information security clauses and clauses required by law[2] where those agreements include the processing of personal data on KCC's behalf. It is important to check whether these are followed and in some circumstances KCC has a right in law to review the contractor's evidence of compliance[3].

What are my responsibilities as an employee?

Employees are expected to understand the importance of protecting information, put KCC's policies and procedures into practice and keep up to date with information governance campaigns on KNET.

Staff must not try to bypass security measures, for instance by storing work in their own online accounts or using a colleague's login. It may be a criminal offence to deliberately try to access or disclose information without authority.

What should I look out for?

Criminals aim to deceive (e.g. pretending to be someone or sending "phishing" emails). Minimise risks through vigilance and caution.

When sending personal information by either post or email, check it is going to the right recipient. If using mail-merge, check it has been done properly before sending.

Business continuity is important. Have plans in place to maintain, restore and recover services when things go wrong.

What if there is a breach or loss? Report information security incidents using the Data Breach Policy. Incidents are handled sympathetically and aim to learn lessons rather than apportion blame.

[1] Management Guide 5 – Information Governance – I don't think that this exists anymore and has been taken down off Knet?
[2] Article 28(3) GDPR
[3] Article 28(3)(h) GDPR – where the contractor is a 'processor' of KCC's information

1. Introduction

This policy sets out core Information Security principles that ensure KCC can meet its legislative and regulatory obligations and maintain its reputation as a professional and trustworthy organisation. Information is essential to KCC's business and consequently must be protected. Information is held in a wide range of digital and physical formats. However, information is processed, shared or stored, it should be protected in an appropriate way.

In an increasingly connected environment, KCC’s information faces an increasing number and variety of threats. Information security provides the technical and organisational measures needed to protect the privacy and confidentiality of our employees and those we serve.

With the advent of the General Data Protection Regulation (GDPR) in May 2018, significant new laws have been introduced that give individuals more rights to be informed about how KCC is using their personal data and a greater duty on KCC to ensure every aspect of its data handling is carried out lawfully, fairly and transparently, with significant fines for getting it wrong. KCC recognises that it must be accountable and proactive to ensure the integrity and confidentiality of personal information and to embed and evidence a privacy culture.

2. Aims

The aims of this policy are to:

- Maintain KCC’s legal and regulatory compliance for data protection;
- Meet the privacy and confidentiality expectations of its residents and partners;
- Appropriately protect personal, confidential and sensitive information;
- Minimise security incidents and breaches;
- Embed a culture of security and an awareness of the need for privacy ‘by design and default’[4].

3. Scope

This policy applies to personal and business information created or processed by or on behalf of KCC in pursuance of its powers and functions. Information may be held or processed in digital, electronic or paper formats using any device or means of transfer.

4. Policy statement

KCC seeks to promote a culture that properly values, protects and uses information for the public good. Information security is part of KCC’s wider information governance management and policy framework.

KCC applies a risk management approach to information security. This identifies information assets on which KCC is dependent and assesses risks to their confidentiality, integrity and availability. Appropriate and proportionate technical and organisational controls are applied to minimise these risks; these include the way KCC is organised, its policies and procedures and the way technology is used.

[4] Article 25, GDPR

Personal data is protected in accordance with the principle of ‘integrity and confidentiality’ as required by the GDPR.[5]

4.1 Principles

(a) Information security is part of KCC’s wider information governance management and policy framework[6] and the approach is based on published good practice[7].

(b) KCC defends its information against common threats such as opportunistic hackers and abuses of business processes, while remaining proportionate and aligned with wider business goals.

(c) KCC’s risk-management approach to information security[8] assesses risks to the confidentiality, integrity, availability and resilience of information and to the processes and services involved in the processing of that information.

(d) KCC takes into account the nature, scope, context and purposes of processing personal information as well as the likelihood and severity of any risks involved to the rights and freedoms of individuals[9].

(e) KCC implements measures to ensure a level of security appropriate to the risk, including:

- the pseudonymisation and encryption of personal data
- capability to facilitate the availability and access to personal data in a timely manner in the event of a physical or technical incident
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[10]

(f) Information security controls are based on ISO27002 (Code of Practice for Information Security Controls) such that they consider:

i the sensitivity and value of information

ii the impact or harm that may result should an incident or event occur.

(g) Managers are responsible for ensuring that those handling personal and confidential information are competent to do so and are supported by robust policies and procedures.

(h) Contractors are held to account under contract terms required by law for their handling of KCC’s personal and confidential information.

(i) Personal and confidential information are only to be shared with external partners in ways that are secure, fair, transparent and lawful.

(j) KCC responds promptly and effectively to information security incidents and has a Data Breach Policy to ensure all personal data breaches are notified appropriately and without undue delay[11].

[5] ‘Article 5(1)(f)

[6] Information Governance Management Framework (Rev 2018)

[7] https://www.nlawarp.net/wp-content/uploads/2018/04/GDPR-V5-Final.pdf

[8] In compliance with Public Service Network certification.

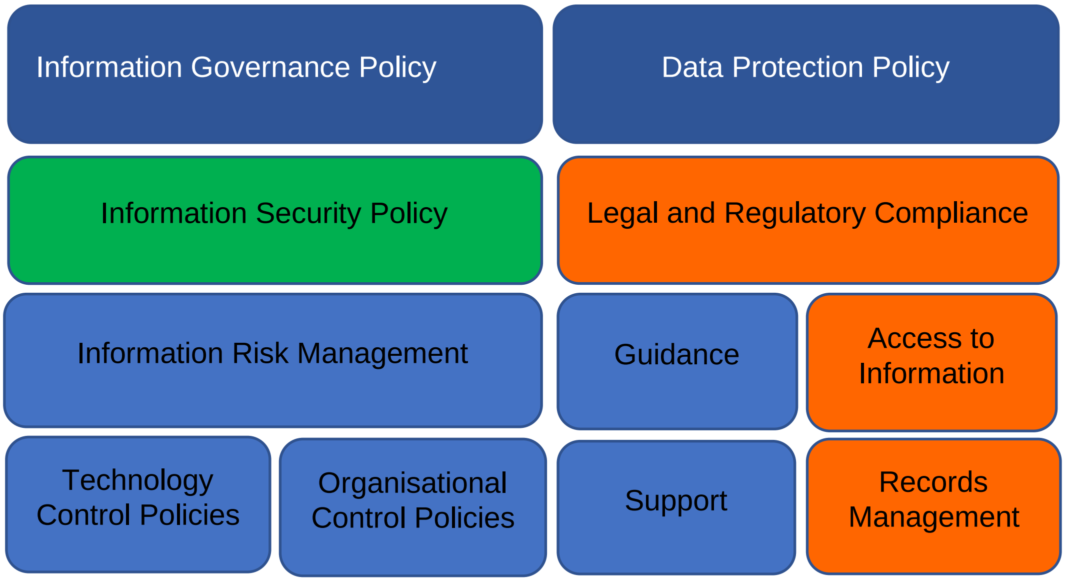
[9] Article 32(1) GDPR

[10] Article 32(1)(a) – (d)

[11] Article 33(1) GDPR – and not later than 72 hours after having become aware of it

4.2 Policy framework

(a) This Information Security Policy is one of a suite of policies which sit under the overarching Information Governance and Data Protection Policies. It sets out the process by which threats to KCC's information security are identified and controlled. It should be read in conjunction with KCC's Data Protection Policy.


Information Governance Policy
Data Protection Policy
Information Security Policy
Legal and Regulatory Compliance
Information Risk Management
Guidance
Access to Information
Technology Control Policies
Organisational Control Policies
Support
Records Management

(b) Subordinate control policies apply to specific risks and these can be found on KNET[12].

4.3 Roles and responsibilities

(a) KCC's Governance and Audit committee is responsible for reviewing the adequacy of information risk management and its governance.

(b) Information security roles and responsibilities are described in KCC's Information Governance Management Framework[13] and include:

(i) The Corporate Risk Manager

(ii) Data Protection Officer (DPO)

(iii) Senior Information Risk Owner (SIRO)

(iv) ICT Compliance and Risk Manager

(v) Information, Resilience & Transparency Team (IR&T)

(vi) Information Governance Cross-Directorate Group

(c) The Corporate Risk Manager is responsible for reporting corporate risk in accordance with KCC's Risk Management Policy and Strategy 2019-2022[14].

(d) The Data Protection Officer (DPO) is responsible for informing and advising KCC and staff on the obligations under the GDPR, for monitoring compliance with the GDPR and for providing advice on data protection impact

[12] https://kentcountycouncil.sharepoint.com/sites/KNet/Pages/policies.aspx

[13] Information Governance Management Framework (Rev 2018)

[14] available on KNET

assessments (DPIAs). The DPO is also the contact point for the ICO on any issues relating to data processing carried out by KCC.

(e) The Senior Information Risk Owner (SIRO) is responsible for providing assurance to KCC that information risks are adequately controlled.

(f) The Information Governance Cross-Directorate Working Group maintains the Information Risk Register and monitors information security incidents and residual risks. It has the authority to issue risk control notices where risks are elevated.

(g) Managers are required to comply with the Managing Risk Toolkit.

4.4 Information risk management

Information risk is managed by the SIRO who has corporate oversight of information risks associated with KCC's information assets. Corporate Directors are responsible for managing risks associated with assets within their service areas.

a. Information assets

For management purposes each key business information system is an 'information asset'. Each asset is accredited[15] as meeting KCC's information security requirements, either at service commencement or through a documented information risk assessment.

The Records Manager[16] is responsible for maintaining the Corporate Information Asset Register (CIAR) for the SIRO and the Register of Processing Activities (ROPA) for the DPO. The ICT Compliance and Risk Manager is responsible for ensuring each asset is accurately documented with:

(i) technical overview and description

(ii) details of contracted third parties who manage or provide the asset

(iii) information risk assessment

(iv) risk-review statements.

(v) the assigned Information Asset Owner (IAO) and Information Asset Administrator (IAA).

b. ICT information risk assessment

(i) ICT Information risk assessments must be completed by a 'competent person'[17]. Assessments can be ordered from the ICT service desk.
(ii) Residual information risk(s) that exceed corporate risk tolerances after recommended controls are implemented must be considered by the relevant IAO.
(iii) ICT Information Risk Assessments are held by the ICT Compliance and Risk Manager who also schedules annual risk statements.
(iv) Risk Assessments and summary risk statements are sent to Information Asset Owners.

[15] ST INF Risk and Compliance Team

[16] ST GL Information Resilience and Transparency Team

[17] BCS Certified Information Risk Practitioner or equivalent

c. Data privacy by design and default

i. The GDPR requires data protection to be carried out 'by design and default'. This means appropriate technical and organisational measures (such as pseudonymisation) that effectively implement data protection principles (such as data minimisation) and that safeguard the data must be taken into account both at the time of design and when new systems or processes are implemented.

ii. All measures should ensure that only personal data that are necessary for each specific purpose of the processing are processed. This applies not just to the amount of data collected, but also the extent to which that data is processed, its accessibility and storage period.

d. Data protection impact assessments

Where any processing is likely to result in a high risk to the rights and freedoms of individuals, a data protection impact assessment should be carried out. This acts as evidence that KCC is complying with its obligations under the GDPR and must be conducted when systems are planned which involve:

- systemic and extensive profiling, which has significant effects on individuals
- processing of special category data or personal data relating to criminal convictions or offences on a large scale.
- systematic monitoring of public areas (e.g. CCTV)
- using new technologies (or novel application of existing technologies)
- profiling or special category data to decide on access to services
- profiling of individuals on a large scale
- processing of biometric or genetic data
- data matching or dataset combining from different sources
- collection of personal data forms a source other than the individual without providing them with a privacy notice
- tracking individuals' location or behaviour
- profiling children or targeting marketing or online services at them
- processing data that might endanger the individual's physical health or safety in the event of a security breach.

Other criteria may indicate a high risk and should be considered prior to processing the information. Further information is contained in KCC's Data Protection Impact Assessments Policy and Guidance.

4.5 Secure data handling

Most routine handling of personal and sensitive information uses digital applications and services provided by KCC's ICT service provider(s) and is designed with appropriate security (paper records are covered later). Information sent or moved beyond KCC's network is likely to leave its security control. There are legal restrictions on when and how personal information can be shared. In all personal data handling KCC must have a lawful basis to process personal information as set out in its privacy notice(s). If in doubt seek advice from IR&T or the DPO.

(a) If sending personal or sensitive information, check the recipient's address. If using email comply with the Secure Email Policy[18] and the Specialist Guidance in the Information Management Manual on Managing Email. If using another method, ensure it is secure. If in doubt, seek advice from line managers.

(b) If communications are generated by an automated IT system, or mail-merge is used, check before sending to ensure the right recipient receives the right information.

(c) Those sending personal or sensitive information must be competent to do so and have completed mandatory data protection and information governance training.

(d) Those sending personal or sensitive information must be confident that the recipient is capable of and undertakes to handle the information in a secure and proper manner.

(e) Managed printers have 'follow-me' features mean that documents are only printed in the presence of the authorised user, reducing the risk of being left unattended or sent to the wrong printer.

(f) Those handling personal or sensitive information must have regard to the safeguards and controls set out in KCC's Information Management Manual, in particular the sections covering Information Security, Retention and Disposal.

(g) Those receiving personal or sensitive information from external sources (for example CJSM or Public Health) must handle the information in accordance with the terms and conditions of its use. In accordance with the Terms and Conditions of use of the Ministry of Justice's CJSM service, all CJSM users must ensure that the following handling instructions are added to the footnote or signature of their emails:

'*The information in this email is classified as OFFICIAL as defined in the Government Security Classifications (GSC) Policy. That means that this email contains official and personal information, some of which may be sensitive information, which MUST be stored and disposed of securely, only used for the purposes for which it was provided, and in accordance with the Ministry of Justice's terms and conditions of use of the CJSM service. This information must not be transmitted onwards without additional assured protection (i.e. by only sending to another authorised user on a strict need to know bass via CJSM) or via the Public Services Network – this includes the domains gsi.gov.uk, pnn.police.uk, justice.gov.uk and nhs.net)*.'

(h) Those handling personal or sensitive information should use measures such as pseudonymisation and encryption where appropriate.

4.6 ICT security

KCC's ICT systems and services are certified by the Public Service Network Agency as appropriate for OFFICIAL classified information. This requires policies designed to

[18] http://knet/ourcouncil/Key-documents/Documents/Secure email policy.pdf

control specific risks relating to ICT security; these can be found on KNET under relevant headings[19]. The following highlights those applicable to most users.

(a) Access to KCC's ICT systems must be authorised by an appropriate manager. If an employee, this will be their line manager. If a contractor this may be the relevant contract manager.

(b) All employees are required to comply with the ICT Acceptable Use Policy as a condition of service.

(c) Users are responsible for keeping their password secure and must not disclose or share it. Employees are accountable for activity on their user account.

(d) Most data breaches are caused through negligence (insider threat) and training and awareness raising are the best line of defence to reduce this. Think before you click.

(e) Screens must be locked when employees are away from their computers.

(f) KCC's mobile devices must be cared for and not left unattended in public places or visible in a parked car. If using a personal device, staff must not circumvent controls that are in place to protect KCC's information. Staff must abide by KCC's BYOD Policy. Staff must report any loss or theft promptly.

(g) Staff must follow the Using IT Equipment for Remote Mobile Working Policy[20] and the specialist guidance in the Information Management Manual[21] on removing physical records from KCC premises and on working away from the office together with associated guidance on KNET.

(h) When storing data electronically outside of KCC's server environment, staff must abide by the council's Safe Use of Removable and Online Storage Policy.

(i) Where cloud services are being used, it is essential the personal data is stored within the EU or other recognised domain using the ICO model clauses or based on an EC 'adequacy decision'[22] and following cloud security principles. Staff should refer to the Safe Use of Removable and Online Storage Policy for further information.

4.7 Physical and environmental security

The physical and environmental security of KCC's buildings and premises is managed by facilities contractors. Managers are responsible for the training and security policies and the practices of their employees.

(a) ID cards must be worn, and visitors issued with a temporary pass and escorted during their visit. Those not wearing badges or seen 'tailgating' should be challenged.

(b) Desks must be clear of personal and sensitive information when unattended or outside of normal working hours. Documents containing personal or sensitive information must be locked away when not in use.

[19] Audit Log Management Policy, ICT Asset Management Policy & Guidance, Master Service Administrator Accounts Policy, Software Update and Patch Management Policy; User Identification and Authentication Policy & Standard; Using Remote Support/Administration Software Policy.

[20] http://knet/ourcouncil/Key-documents/Documents/Using IT for **Remote** Mobile **Working** Policy.pdf

[21] http://knet/ourcouncil/Documents/InformationManagementManualV03.pdf

[22] Article 45

(c) Managers should undertake periodic confidentiality surveys[23], the results of which should be used to inform improvements.

(d) Areas where Confidential Information[24] is processed or handled should be treated as Safe Havens[25].

(e) Paper records may be vulnerable to environmental risks such as water or fire or may be left in abandoned buildings. The risks to paper records should be assessed periodically and when significant change to the physical environment are proposed.

(f) The physical and environmental security of ICT equipment (not user devices) is assessed at installation and reviewed annually.

4.8 Mobile and remote working

Employees who access their work away from the office must do so within the terms and conditions of the Using IT Equipment for Remote Mobile Working Policy and Standard.[26]

4.9 Employment starters and leavers

(a) Appropriate background checks are carried out during recruitment (including temporary workers) and prior to appointment, with vetting for sensitive and regulated roles.

(b) A checklist and guidance for managers and those employing contractors ensures all new starters complete mandatory training, including information governance and data protection (GDPR) modules.

(c) All new employees sign to confirm they understand their employment Terms and Conditions (Blue Book) and the Kent Code (Code of Conduct). Both documents include sections on information security.

(d) Managers must authorise access to ICT systems and services, and for sensitive applications, additional training is mandatory before access is approved.

(e) Managers requesting user accounts for temporary workers must provide an end date. Access to ICT services is automatically revoked when temporary workers reach this end date unless expressly renewed by the line manager requesting an extension.

(f) Whether accidental or deliberate, employees and contractors can pose a potential threat to the security of KCC’s information. They may be disgruntled, politically or religiously motivated, or subject to financial or personal pressures. The line manager is best placed to pick up and act on indications that may cause concern and respond appropriately.

(g) A checklist and guidance for managers ensures that user accounts are rendered inaccessible when an employee or temporary worker leaves employment. Managers must ensure that when staff leave or move to new roles the access rights of those staff are updated.

[23] Contact the Information Resilience and Transparency Team for more information.

[24] Relating to an individual’s health or adult social care (HASCA 2012 s263)

[25] Code of Practice on Confidential Information (HSCIC 2014)

[26] ICT Mobile and Remote Working Acceptable Use Policy

4.10 Training and awareness

(a) KCC offers appropriate training, information, advice and guidance to ensure employees are aware of their personal responsibilities in respect of information security and are competent to carry out their duties.

(b) All employees, including temporary and contract must complete mandatory information governance and data protection training during induction. This is recorded on their HR record (employees) or on Delta (temporary and contract staff).

(c) Information governance training is refreshed every other year. Non-completion is reported to the relevant line manager for action. Persistent non-completion is reported to the appropriate Director and the line manager held accountable for ensuring it is completed.

(d) Additional training needs may be identified for specialist roles and professions. These are dealt with in divisional learning and development plans or in individual training plans.

(e) Senior Information Risk Owner (SIRO), Information Asset Owners and Caldicott Guardian roles must receive specialist training within six weeks of their assignment.

(f) KCC will support the DPO by providing the resources necessary to maintain the required standard of expert knowledge.[27]

(g) Only trained 'competent persons' can assess risks to the council's information assets.

(h) Training must be recorded on an individual's employee record and be available in a way that allows corporate and regulatory oversight (i.e. the ability to produce aggregated reports and statistics and on demand by the ICO).

(i) It is the responsibility of line managers to ensure employees moving or changing roles are made aware of local operating procedures.

4.11 Business continuity

Business Continuity Plans should be in place for all critical information assets with relevant employees aware of their roles and responsibilities.

4.12 Contractor assurance

(a) Contracted services frequently process personal, confidential or business information on KCC's behalf. Information security and data protection legal clauses are included in all standard contract terms and conditions. Where these standard terms and conditions are not used, equivalent clauses must be included. All contracts involving the processing of personal data on behalf of KCC must contain the minimum stipulations required by the GDPR[28]. These are:

- the organisation may only act on the written instructions of KCC
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of KCC and under a written contract
- the organisation will assist KCC in providing subject access and allowing individuals to exercise their rights in relation to data protection

[27] Article38(2)

[28] Article 28 GDPR

- the organisation will delete or return all personal information to KCC as requested at the end of the contract
- the organisation will submit to audits and inspections, provide KCC with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell KCC immediately if it is asked to do something infringing data protection law.

(b) Contract managers are responsible for monitoring contract performance, including data protection compliance and must be able to provide evidence of this. They should refer to ICO guidance for further information.[29] Any of the following evidence may be considered:

(i) if a contractor demonstrated during procurement that it has appropriate technical and organisational measures in place to ensure a level of security appropriate to the risk of any personal data processing[30]

(i) whether the contractor holds a recognised information security accreditation such as ISO27001 or Cyber Essentials+

(ii) if a health or social care provider, whether they hold a 'satisfactory' or better IG Statement of Compliance (NHS Data Security and Protection Toolkit)

(c) Where a contractor is unable to demonstrate that their information security measures are adequate, restrictions must be considered, such as the use of secure email, until improvements are made. A failure to ensure a contractor has adequate security measures in place as required by the GDPR[31] exposes KCC to the risk of a significant fine of up to 10 million Euros.[32]

4.13 Information sharing

Information sharing must be carried out in accordance with KCC's Information Sharing Policy. In summary this means:

(a) all sharing of personal data must be fair, lawful, transparent and properly documented

(b) the data transfer must either be via an existing secure service or using an agreed and risk-assessed approach.

KCC is a signatory to the Kent and Medway Information Sharing Partnership Agreement (KMISP) and this agreement should be regularly reviewed by staff to ensure it is being followed appropriately.

4.14 Information security incidents

KCC has an incident reporting system that must be used promptly when reporting information security incidents as set out in the Data Breach Policy. Serious incidents should be raised immediately with line managers who can inform the SIRO, IAO or relevant Director.

[29] https://ico.org.uk/media/aout-the-ico/consultation/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

[30] Article 32 suggests these include pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

[31] Article 28(3)(c) and Article 32, GDPR

[32] Article 83(4)(a)

5. Monitoring

Information security is monitored and reported through the following:

(a) Information Governance Cross-Directorate Group

(b) internal audit.

There is an annual cycle of audits that cover areas of the business deemed to represent the greatest risk to the council. This includes information security and risks are reported to the Governance and Audit Committee.

(c) Data Breach Register[33]

This is owned and monitored by the DPO as part of the role's compliance duty[34].

6. Policy review

This policy will be reviewed annually.

7. Information, advice and guidance

7.1 IG documents and guidance can be found on the KNET Information Governance site, or in the Information Governance Toolkit, also on KNET

7.2 Advice on Information Security and Information Risk Management can be obtained by contacting the Infrastructure Compliance and Risk Manager kathy.stevens@kent.gov.uk

7.3 Advice on Records Management can be obtained by contacting the Records Manager by email elizabeth.barber@kent.gov.uk.

7.4 Advice on data protection can be obtained from the DPO or the Information Resilience and Transparency Team. E: dataprotection@kent.gov.uk.

8.Associated policies and documents

- Data Protection Policy
- Information Governance Policy
- Information Governance Management Framework
- Data Breach Policy
- Anonymisation and Pseudonymisation Policy
- Information Sharing Policy
- Records Management Policy
- Information Management Manual
- Secure Email Policy
- Safe Use of Removable and Online Storage Policy
- BYOD Policy
- Using IT for Remote Working Policy
- Audit Log Management Policy
- ICT Asset Management Policy
- Master Service Administrator Accounts Policy
- Software Update and Patch Management Policy
- User Identification and Authentication Policy & Standard
- Using Remote Support/Administration Software Policy
- ICT Acceptable Use Policy

[33] Article 33(5) GDPR
[34] Article 39(1)(b) GDPR

- ICT User Standards Policy
- Kent Code
- Work Smart (Flexible Working) Policy
- Data Protection Impact Assessment Policy and Guidance
- Kent & Medway Information Sharing Agreement