Information Governance Policy

*Keepinginformationaboutcustomersandemployeess afe
andsecureandusingittohelpimprovetheserviceswe
provide.*

_____

Version: V0.1 DRAFT
VersionDate: October2020
RevisionDate: October 2022

PolicyStatement

This Policy establishes the key high-level principles of information governance and data protectionin Walsall Council. It provides an overarching direction that ensures all staff are aware of their duties and obligations as set out by the Data protection Regulations and Legislation by ensuring, all staff are fully supported through a framework of Information Governance Standards, Procedures and Guidancethat are embedded into our working practices and data processing activities.

This Policy and the Information GovernanceStandards, Procedures and supporting Guidanceapplytoallemployees,electedmembersandanyoneelse workingfororonbehalf ofthecouncil i.e. partners,contractorsandagents.

Tothisend,
thecouncilcommits
to:

Information Governance Management: supporting robust operationalandmanagementaccountabilitystructures,withappropriatereso urces andexpertisetoensure information governance and data protection compliance issuesaredealtwithappropriately, effectivelyandatlevelswithintheorganisationcommensuratewiththetypean d gravityoftheissueinquestion.

Staff **Empowerment:** embeddingacultureofindividualresponsibilityandcapability acrossthecouncilinrelationtoinformationmanagement,protectionandusea spartof'businessasusual'.

TrainingandAwareness:maintaining asystemoftrainingandawarenessthat meets governmentand contractualmandatoryrequirements,andis capableofequippingemployeeswiththeskillsandknowledgenecessarytodo theirjobsandrespondtocustomerdemandwhilecomplyingwiththeGeneral Data Protection Regulations 2016, UK DataProtection Act 2018 alongsideInformationand Cyber SecurityStandards or requirements.

SystemsandProcesses:establishingand maintaininginformationsystemsand processestoenabletheefficientandsecurestorageandretrievalofinformatio nandthemanagement ofinformationrisk.

Policyandguidance:developingandembedding,standards, proceduresandguidancedocuments inrelationtotherespectiveareasofinformationgovernancethatsupportempl oyeestofullyunderstandthedutiesandresponsibilitiesrequiredto ensure the council continues to comply with its legal obligations.

1.   Applying the Policy

Inapprovingthis InformationGovernancePolicy,thecouncil recognisesand supports:

- theprinciplethataccurate,timelyandrelevantinformationisalegal requirementand essentialtodeliverhighqualityservicesand thatitisthe responsibilityofanyone working fororonbehalfofthecouncilto ensureandpromotethequalityofinformation and toactivelyuseinformation indecision-makingprocesses
- theneedforanappropriatebalancebetweenopennessandconfidentialityin the managementanduseof information
- thattheprinciplesofcorporategovernanceandpublic accountabilityplace equal importanceon the confidentialityof,and the securityarrangements tosafeguard,both personalinformationabout customers andemployees and commerciallysensitiveinformation
- theneedtoshareinformationwithotherorganisationsinacontrolledandsecu re mannerconsistentwiththeinterestsofthecustomerand,insome circumstances, the publicinterest.

2.   Senior Roles and Responsibilities

TheInformationGovernanceStructureisledbyacorporate group–theForumfor Information Governance &Assurance(FIGA),whichisaccountableto theCorporate ManagementTeam.

MembershipoftheForumconsistsofInformation Championswho holdseniorrolesinthecouncilandseektochampiontheprinciplesand requirementsof informationgovernance acrossthecouncil.

TheForumischairedby theSIROand or DataProtectionManagerand requires attendance by directorate level information champions, legal and HR representatives, the InformationSecurityOfficer, directorate representatives and the information governance and assurance officersalongsideany other representationas required or appropriate forensuringcompliance oftheregulationsisupheld.

FIGAisresponsiblefor ensuring that Information Governance Policies, Standards, Procedures or Guidance are reviewed and maintained as well asensuringthatanyInformation risksidentifiedareaddressed and actioned accordingly.

The group also provides assuranceto theChiefExecutive,CorporateManagementTeamandelectedmembers thattheorganisationtakesinformationmanagementand governanceseriouslyandcan demonstratevisibleimprovementsthrougharisk-basedapproach and regular reporting requirements, which ensure appropriate levels of accountability are in place throughout the council.

Roles	Responsibilities
SeniorInformationRiskOwner (SIRO)	Is accountable for information risks, fostering a culture for protectingandusingdataappropriatelyandprovidessenior responsibilityformanaginginformationrisksandincidentsand isconcernedwith themanagement ofall informationassets.
Caldicott Guardian	Isadvisoryand actsas theconscience of theorganisation. Providesafocal point forcustomerconfidentiality&informationsharingissue s. Isconcerned with the managementandsharingofpersonal information.
DataProtection Manager	The DataProtection Manager ensuresthat the council has adoptedgoodinformation governancepoliciesandprocedures andcomplieswithdataprotectionlaws. Thisfunction willalsoactin anadvisorycapacity totheChief Executive, CaldicottGuardianandSIROwere required.Thisfunctionwillbedeliveredthroughtheroleofthe'DataPr otectionManager',whichalsoactstheDataProtectionOfficerfor thecouncil in itsstatutoryfunction.
InformationSecurity Officer	Responsible for developing,implementingandreviewing policiesandprocedurestoprotectthecouncilsnetworkand informationassets,providingadviceand guidanceon informationand cyber security.The rolewillalsoinputinto generaluserawarenessandtrainingandisresponsiblefor dataand cyber security initiatives generally.
InformationGovernanceand Assurance Officer(s)	Responsible for developing, implementing and enforcing policies and procedures to ensure correct information and recordsmanagementpracticeacrossthecouncil.Delivering reports to FIGA that cover the requirements for data processing, information assets, and assessment/audit outcomesalongsideregulatorycompliance.Theroleisalso responsible for ensuring compliance with information governanceawarenesstrainingandthedeliveryofappropriate training throughouttheauthority.
InformationChampions	This role is responsible for ensuring data protection breaches are managed and directorates are accountable for any required actions or risks identified though the incident management process. They act as the key link between the information governance team and the directorate senior leaders to ensure that the councils remains compliant with its legal duties and responsibilities for accountability. They Championdata protection awareness,understandingandcompliancewiththe keyprinciplesofinformationgovernance within the directorate. As membersofFIGA they are responsibleforensuring key messagesand actionsare disseminatedappropriatelythroughout thedirectorates.
InformationAsset Owners	Accountableseniorofficerswith ownership and responsibilityfor informationassets(paper based and electronic records and IT systems) within their directorate.IAO'smust identifyanddocument within the information asset register, the availabilityand compliance requirementsfortheir systemsandformulatea contingencyplanin theeventofsystemfailure. Supportedby

InformationAssetCustodians	Designated officer with responsibility for day-to-daymanagement, administration andprotectionof specified information assets(paper-basedrecordsand IT systems).

3.   Strategic Implementation

FIGA will monitorimplementationofthisPolicyand associated documentsthroughregularmeetings, whichwill involve:

- ensuringany Standardsand procedures or guidancerequired for compliance of obligations are developed, reviewed and monitored while being responsible for the approval ofthesedocuments through the directorate leads and champions.
- ensuringappropriateresourcesareinplacetoachi evecomplianceoftheregulatory requirements
- reportingonprogress, incidentsandissues to accountable senior level positions including CMT/electedmembers.

ThisPolicywillbereviewedbienniallyandapprovedbyFIGA,CMT and thecouncil'sfull Cabinet.

4.   Governance and Compliance

Non-compliancewiththisPolicy and the associated Information Governance standards, procedures or guidancecouldpotentially exposethe council and/or its customers to significant levels of risk. The potentialimpactof such risks through the damage, unauthorised disclosureor loss of information includes but is not limited to:
- disruptionto services,
- the riskof harm or distress tocitizens,
- damage tothe organisational reputation,
- legal action,
- monetary penalties,
- personaldistress,
- lossofconfidence,
- ormediacoverage

andmay take considerable timeandcosttorecover from.

5. Responsibilities

The Data Protection Manager shall have overall responsibility for managing and implementing theInformation Governance Policy and accompanying Standardsandproceduresona day-to-daybasis.

Line Managers are responsible for ensuring that their permanent and temporary employeesandcontractorshave:-

- readandunderstoodthe Information GovernancePolicyandtheStandardsandproceduresapplicable in theirworkareas
- beenmadeawareof theirpersonalresponsibilitiesanddutiesinrelationto informationgovernance
- been madeawareofwho tocontactfor further advice and where to locate any guidance
- receivedappropriate and up-to-datetraining relating to information governance
- abidebythecouncil'sCode ofConduct

Line Managers are also responsible for ensuring that any information or data processing undertaken by their service area or team complies with both the data protection and records management requirements or standards and that staff have been made aware of the top level principles of good information governance in that records must be:

- Adequate, relevant and not excessive
- contain the minimum information required for the specified purpose
- that appropriate privacy notices ensure transparency over any data processing activity
- justified, lawful and available on a need to know basis only

All staff are responsible for ensuring that they comply with the data protection principles and standards in that they are directly responsible for respecting and upholding confidentiality, using information for the purpose for which it was collected and sharing or accessing information in a secure and adequate manner on a need to know basis only.

All Staff must comply with the Standards, Procedures and Guidance that is part this policy

Non-compliancewiththis policy and the Information Governance Standards, Procedures or guidance maythereforebesubjectto performance or disciplinaryaction,inlinewith thecouncil'sdisciplinaryprocedures andor legalactionifappropriate.

The followingtableidentifieswhowithinWalsallCouncilisAccountable, Responsible,InformedorConsultedconcerningthisPolicy. The following definitionsapply:

- **Accountable**– thepersonwhohasultimateaccountabilityandauthorityforthePolicy.
- **Responsible**–theperson(s)responsiblefordeveloping andimplementingand reviewingthePolicy and any associated Standards, procedures or Guidance.
- **Consulted**–theperson(s)orgroupstobeconsultedwhenthePolicyis reviewedandapproved
- **Informed**– the person(s)orgroupstobe informedthroughouttheapproval process.

Accountable	SeniorInformationRiskOwner
Responsible	DataProtectionManager
Consulted	ForumforInformationGovernance&Assurance(FIGA)
Informed	Allindividualsemployedbythecouncileitherpermanently,ona temporarybasisorasacontractor,electedmembersandpartner organisations

Document History

Revision Date	Version	Revised By	SummaryofChanges
19/10/2020	0.1 Draft	C. Hobbs	Policy extracted from Information Governance Framework Standards 2018.
30.10.2020	0.1 Draft	P.Withers	Policy amended and edited to ensure responsibilities and duties align to the legal requirements.

1. Approvals

ThisPolicy has received the following approvals:

Name	Title	Signature	Dateof Approval
Forumfor InformationGovernance &Assurance (FIGA)		As minuted	27.10.2020
Corporate Management Team (CMT)			
Cabinet			

Appendix 1 – Legal Requirements, Regulations andStandards

Thecouncil and all individualsworkingfororonbehalfofthecouncilaregoverned bya number oflaws,regulationsand standardsrelatingto informationgovernance. These include but are not limited to:

- Accessto Medical Records Act 1990
- CaldicottReview2017
- CCTV Code of practice 2017
- CCTV Code of conduct 2019
- Children and Families Act 2014
- Civil EvidenceAct1995
- Code ofpracticefor legaladmissibilityand evidential weightofinformationstored electronically BIP0008:2014
- Commonlawdutyofconfidence
- ComputerMisuseAct1990
- Copyright, DesignsandPatents Act 1988
- Data Protection Act 2018
- Environmental Information Regulations2004
- FreedomofInformationAct2000
- General Data ProtectionRegulations(GDPR)2016
- Health and Safety atWorkAct1974
- Health and Social CareAct2001
- HMGSecurity PolicyFramework2014 (v1.1 May 2018 to take account of GDPR)
- HumanRights Act 1998
- International StandardforInformationandDocumentation,RecordsManagement
- InternationalStandardsforInformationSecurity-ISO27001:2013&ISO27002:2013
- Investigatory Powers Act 2016
- ISO 15489 Records Management Code ofPracticefor Health and Social Care2016
- ISO 27001InformationSecurityManagement Standards
- ISO 27032:2012Information technologySecuritytechniques-Guidelinesforcyber security
- Local GovernmentAct 1972 (Section224)
- Mental Capacity Act2015
- NHS Confidentiality Code ofPractice 2016
- PCI/DSS
- Safeguarding Vulnerable Groups Act 2006UK DataProtectionAct 2018

6.   Appendix 2 - Related Council Standards, Procedures and Guidance

- Account Access Request Procedure
- Archive Procedure
- <mark>Data Change Request Procedure</mark>
- DataQuality Procedure
- Dealingwith Subject Access Requests(SARs)Procedure
- E-mail &Internet Usage Procedure
- Email Retention – A Quick Guide to Managing Emails
- HandlingPersonIdentifiable Data
- InformationClassification Procedure
- <mark>InformationRisk and Security Standard</mark>
- Mobile Device Acceptable UseProcedure
- Naming ConventionProcedure
- ProcedureforReportingand ManagingData Breaches
- Protective MarkingProcedure
- <mark>Records Management Standards</mark>
- Use ofRemovable Media Procedure
- VersionControl Procedure
- Agile Working Policy
- Information Risk and Security Standard
- Records Management Standard
- Data Protection Standards