Mae'r ddogfen hon hefyd ar gael yn Gymraeg

This document is also available in Welsh

GIG CYMRU NHS WALES Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** PHW92 **Version Number:** 1 **Date of next review:** March 2029

Digital Supplier Management Policy

Policy Statement

Public Health Wales is committed to ensuring that all digital, data, and technology procurement activities are conducted in a transparent, secure, and sustainable manner. This policy establishes the governance framework and minimum standards required to procure digital systems, services, and assets that support organisational objectives, comply with applicable legislation, and deliver value for money. It promotes ethical supplier management and ensures that digital procurement contributes positively to public health outcomes, operational resilience, and the wellbeing of future generations in Wales.
This policy is aligned with Public Health Wales' Digital and Data Strategy and supports wider strategic procurement objectives to ensure interoperability, sustainability, and future-proofing of digital investments.

Policy Commitment

This policy sets the governance, controls, and minimum standards for the procurement of digital, data, and technology (DDaT) systems, services, and assets. It ensures compliance with applicable legislation and Welsh Government guidance while promoting transparency, value for money, security, privacy, sustainability, accessibility, and ethical employment throughout the supplier management lifecycle.

Scope

This policy applies to all Public Health Wales (PHW) staff, contractors, and third parties undertaking or influencing digital procurement and supplier management, including:

- Software (on-premises and SaaS), platforms, and licenses
- Hardware, end-user devices, peripherals, and infrastructure
- Cloud services (IaaS, PaaS, SaaS) and managed hosting
- Data platforms, analytics, AI/ML solutions, and integrations
- IT Operations & Cybersecurity solutions, tooling, and managed services
- Digital consultancy, support, and professional services

- Software as a medical device (SaMD)
- All Health IT Systems

Non-digital goods and services are governed by Public Health Wales' general procurement policies and procedures. This policy applies in addition to those policies for any procurement that includes a digital component (e.g., equipment with embedded software or connectivity).

Supporting Procedures and Written Control Documents

All corporate policies and procedures are available on the Public Health Wales website

- Digital Assurance Procedure
- Information Governance Policy
- Information Security Policy
- Data Privacy and Impact Assessment Procedure

Scope

Outline who the policy is applicable to and who the intended audience is. Also use this section to clarify what the policy covers, including any areas that are outside the scope of the document

For example:

This policy applies to all of our staff in all locations including those with Honorary Contracts.

Impact Assessments	An Equality, Welsh Language and Health Impact Assessment has been completed and can be viewed on the policy webpages.
Approved by	Audit and Corporate Governance Committee
Approval Date	10/03/2026
Review Date	10/03/2029
Date of Publication:	06/05/2026
Group with authority to approve supporting procedures	Leadership Team
Accountable Executive Director/Director	Director of Research, Data and Digital and Senior Information Risk Owner
Author	Lead Cyber Security Manager

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Board Business Unit.

This is a controlled document, the master copy is retained by the Board Business Unit

Whilst this document may be printed, the electronic version posted on the internet is the master copy. Any printed copies of this document are not controlled. This document should **not** be saved onto local or network drives but should always be accessed from the internet.

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments**
1		10/03/26	06/05/26	

Introduction

Public Health Wales recognises the critical role that digital, data, and technology (DDaT) systems play in delivering high-quality public health services and supporting organisational objectives. As technology evolves, the procurement of digital solutions must be undertaken with a clear focus on transparency, security, sustainability, and compliance. This policy provides a governance framework that ensures all DDaT procurement activities align with Welsh Government guidance, relevant legislation, and organisational values.

The purpose of this policy is to establish minimum standards and controls for procuring digital systems, services, assets and to support robust contract and supply chain management practices. It aims to safeguard public resources, promote ethical supplier practices, and ensure that procurement decisions contribute positively to public health outcomes, operational resilience, and the wellbeing of future generations in Wales. By embedding principles of value for money, privacy, accessibility, and sustainability, this policy supports the responsible adoption of technology that enhances service delivery and protects the interests of citizens.

Definitions

- DDaT: Digital, Data & Technology
- DDDA: Digital and Data Design Authority
- STA: Single Tender Action (direct award without competition)
- Public procurement threshold: UK threshold above which a competitive process must be advertised via the relevant national portal
- SRO: Senior Responsible Owner
- CDPS: Centre for Digital Public Services
- Whole life cost: Total cost of ownership across the contract term (purchase, implementation, support, exit/transition, disposal)
- Critical Supplier/Service: A supplier/service whose failure would materially impact safety, operations, finance, data, or reputation
- DCB: Data Coordination Board

Roles & Responsibilities

Chief Executive Officer

- Accountable for ensuring that all procurement activity — whether aligned to the Integrated Medium Term Plan (IMTP) or arising from Business-As-Usual (BAU) requirements — complies with statutory financial duties and supports the organisation's strategic objectives.
- Ensures compliance with Standing Financial Instructions (SFIs) and Standing Orders (SOs).

Director of Finance

- Ensures financial control, value for money, and compliance with thresholds.
- Approves STAs within delegated authority and oversees financial evaluation.

Executive Director of Research, Data and Digital

- Leads Digital Strategy and assures alignment of digital procurements with strategic objectives, enterprise architecture, standards, and roadmaps.
- Ensures digital systems are secure, resilient, accessible, and compliant with UK GDPR, the Network & Information Systems Regulations 2018, and PHW policies.
- Approves all digital procurement proposals prior to initiation. (Above £500,000)

NWSSP Procurement Services

- Provides professional procurement support and ensures compliance with public procurement legislation and PHW procedures.
- Leads appropriate competitive tendering strategies, documentation, and contracts.
- Maintains records of all procurement activities, decisions, approvals, and conflicts of interest in the procurement file.

Information Governance (IG) / Data Protection Officer (DPO)

- Oversees DPIAs, personal data risk and GDPR compliance, data sharing/processing agreements, records of processing, and privacy controls.

Digital Services

- Conducts supplier cyber & IT operational due diligence, security risk assessments, and advises on minimum controls, assurance, and testing to ensure secure, integrated, and resilient IT infrastructure for digital systems, data, and networks.
- Head of Digital serviced and Experience approves all digital procurement proposals prior to initiation. (below £500,000)
- Contracts below £500,000 that are large in scale, high risk, or novel in nature will be referred to the Executive Director of Research Digital & data for approval

Budget Holders / SROs

- Own the business case, funding, and benefits realisation; ensure delivery and contract performance against KPIs and SLAs (where appropriate).

Clinical Safety Officer

- Provide clinical safety oversight for supplier digital systems ensuring compliance with relevant clinical safety standards and reviewing supplier safety documentation where systems may impact patient or public safety.

Policy

Principles

All digital procurements must demonstrate:

1. Alignment with PHW strategic objectives and demonstrably delivery sustainable, measurable benefits for the people and communities of Wales.
2. Transparency & Fairness – open, auditable processes and documentation
3. Value for Money – optimal balance of cost, quality, risk, and sustainability using whole life cost
4. Compliance – adherence to public procurement and information laws, PHW Standing Financial Instructions, and Welsh Government policies and mandates
5. Security & Privacy by Design – proportionate technical/organisational controls and DPIAs where required
6. Sustainability & Social Value – alignment with the Well being of Future Generations (Wales) Act 2015 and ethical employment in supply chains
7. Accessibility & Inclusion – digital services meet WCAG 2.2 AA and Welsh language standards
8. Interoperability & Open Standards – avoid lock in; favour open, standards based solutions.
9. Digital Service Standard for Wales (CDPS)
10. Compliance with Digital Clinical Safety standard – DCB0129 Clinical Risk Management for Manufacturers/suppliers

Procurement Lifecycle & Controls

Initiation & Planning

- All procurement proposals must demonstrate alignment with the Digital and Data Strategy and wider organisational procurement priorities as part of the pre-procurement assessment.
- Engage NWSSP Procurement Services and Digital Services at concept stage.
- Define need, outcomes, whole-life costs, funding, timeframes, and alignment with strategy/architecture.

- Complete pre-procurement assessment covering IT operations, cyber security, Information Governance, legal, sustainability, and delivery risks.
- Confirm market engagement approach (where appropriate) and procurement route.

Minimum Competition Requirements (Thresholds), Single Tender Actions, Evaluation/Award and Frameworks

- As set out by your procurement lead

Onboarding, Implementation & Acceptance

- Complete contract finalisation, Data Processing/Sharing Agreements, and information security schedules.
- For software/hardware: require assurance/testing (e.g., penetration testing evidence, secure configuration, vulnerability management).
- Verify accessibility (WCAG 2.2 AA) and Welsh language and applicable standards requirements before go-live.
- Confirm business continuity/disaster recovery (BC/DR) plans.

Contract Management

- Budget Holder (or Contract Manager) must maintain a Contract Management Plan with KPIs, SLAs, risk/issue logs, service credits, and review cadence.
- Quarterly performance reviews for high-value or critical services; at least annual for others.
- Cyber Security/ Information Governance: annual assurance refresh (e.g., ISO 27001 certificate status, vulnerability/penetration test summary, incident reporting, DPIA review).
- Maintain a central Supplier Register (contract details, data categories, security posture, renewal dates, performance history, sub-contractors use).
- NWSSP oversees and coordinates All-Wales contracts.

Exit, Transition & Renewal

- Each contract must include exit provisions, data portability, IP/licensing, deletion/return of data, knowledge transfer, and transition assistance.
- Begin renewal/competition planning at a minimum 24 months before contract end for high-value & critical services as required by the service.

- Secure asset disposal and data sanitisation (certified) per PHW procedures.

Cyber Security & Information Governance Requirements

All digital procurements must consider digital services engagement as an essential requirement to ensure activities meet proportionate baseline controls, including:

- Risk Assessment: Supplier/service risk assessment aligned to PHW's risk framework.
- Data Protection: Conduct DPIA, data processing/ sharing agreements where applicable; confirm lawful basis, data minimisation, retention, and international transfers controls.
- Assurance: Evidence of cyber maturity (e.g., ISO/IEC 27001 or equivalent controls), secure software development, vulnerability management, incident response, logging/monitoring, and MFA for administrative access.
    - Evidence of conformity to required digital standards
    - Evidence of conformity to relevant Welsh Health Circular(s)
- Cloud & Hosting: Data residency, encryption at rest/in transit, key management, identity integration, backup/restore testing, and tenancy/segregation.
- Third-Party Sub-contractors: Transparency, approval, and flow-down of security/privacy obligations.
- Testing: Security testing appropriate to risk (e.g., application/API testing, infrastructure testing) with remediation before acceptance.
- NIS Compliance: Where applicable, suppliers must support PHW's obligations under the Network & Information Systems Regulations 2018.

Accessibility, Inclusion & Welsh Language

- Digital services must meet WCAG 2.2 AA accessibility standards and be tested with assistive technologies where appropriate.
- Procurements must support PHW's duties under Welsh Language Standards; requirements for bilingual interfaces, communications, and support must be explicitly evaluated and contracted.

Sustainability, Ethical & Social Value

- Apply the Sustainable Risk Assessment (SRA) and include measurable sustainability criteria (e.g., energy efficiency, circular economy, e-waste reduction, end-of-life take-back).
- Cloud procurements should consider provider sustainability reporting and carbon efficiency.
- Suppliers must comply with the Welsh Government Code of Practice for Ethical Employment in Supply Chains.
- Social value outcomes (skills, local supply chain development, fair work) should be specified and measured.

Records, Monitoring & Reporting

- Record all procurement activities, decisions, approvals, and conflicts of interest in the procurement file.
- Maintain a central pipeline and a 1,2,3 year look-ahead for digital contracts.
- Provide quarterly reports to the Audit Committee summarising procurement performance, exceptions (including STAs), assurance status, and key risks.

Deviations & Non-Compliance

- Any deviation from this policy requires prior written approval from the Executive Director of Research, Data and Digital (and NWSSP/Finance as applicable) and must be documented.
- Material non-compliance will be reported to the Audit Committee.

Related Policies, References & Governance

- PHW: Standing Financial Instructions; Standing Orders; Information Governance; Cyber Security; Records Management; Business Continuity; Equality, Diversity & Inclusion, DDDA
- Welsh Government: Code of Practice for Ethical Employment in Supply Chains; Well-being of Future Generations (Wales) Act 2015; Welsh Language Standards, Welsh Health Circulars

- UK: UK GDPR, Data Protection Act 2018 & Data Act 2025; Network & Information Systems Regulations 2018; Public procurement law and guidance
- **DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems**

Review & Ownership
This policy will be reviewed annually or sooner upon significant legislative, strategic, or operational change. The Executive Director of Research, Data and Digital is the policy owner.