Archwilio Cymru
Audit Wales

Digital Transformation

Velindre University NHS Trust

April 2026

About us

We have prepared and published this under section 61(3) (b) of the Public Audit Wales Act 2004.

If you need any help with this document

If you would like more information, or you need any of our publications in an alternative format or language, please:

- call us on 029 2032 0500
- email us at info@audit.wales

You can use English or Welsh when you get in touch with us – we will respond to you in the language you use.

Corresponding in Welsh will not lead to a delay.

Mae’r ddogfen hon hefyd ar gael yn Gymraeg.

Audit Wales follows the international performance audit standards issued by the International Organisation of Supreme Audit Institutions (INTOSAI).

Contents

Audit snapshot

What we looked at

1 We looked at how Velindre University NHS Trust's (the Trust) approach to digital transformation is supporting service improvement. This included its approach to digital strategy, leadership and skills development. We also considered how the organisation manages risks around digital infrastructure, cyber resilience, and Artificial Intelligence (AI). Our work was limited to the Trust only; we did not consider the approach taken by the Trust's hosted bodies.

Why this is important

2 Digital technology is a key enabler to many of the aims of A Healthier Wales. That plan says that new technologies and digital approaches will be an important part of the future whole system approach to health and care.

3 However, achieving digital transformation is challenging. It requires investment, the right infrastructure, and staff engagement and training. Systems need to communicate with one another and organisations must manage ever-growing risks around cyber resilience.

4 Digital transformation is not just about technology, it is about culture and leadership. The boards of NHS bodies have a key role in approving and owning the organisation's digital strategy. Boards also need assurance that digital transformation is being managed safely and effectively, and that investment is securing the intended benefits.

What we have found

5 The Trust recognises that digital transformation is central to modernising its services. While it has a 10-year Digital Strategy with supporting governance arrangements in place, the strategy does not include a detailed, costed delivery plan. This makes it harder for the Trust to prioritise work, use resources effectively, and be confident that its digital goals can be achieved with the capacity it has.

6 Digital investment has increased mostly because revenue costs are rising. However, capital funding is unpredictable and is expected to fall sharply in 2026-27. This creates risks for replacing old systems, which may cause delays in the delivery of the Digital Strategy.

7 National systems are expected to help the Trust improve safety and efficiency, while local projects, such as the Digital Training Platform, user-centred design work, and early use of AI, aim to help staff work more efficiently and supporting more modern ways of working.

8 However, progress is being held back by several gaps in the Trust's arrangements. Key risks linked to cyber security, old systems and AI are not always recorded in a consistent way, which limits the Board's ability to oversee them effectively. The Trust also does not yet have a clear understanding of digital skills across its workforce. In addition, evaluation of digital projects is limited, making it hard to show whether expected benefits are actually being delivered.

What we recommend

9 We have made six recommendations to the Velindre University NHS Trust, which focus on:

- improving how it oversees and tracks digital infrastructure risks;
- increasing the frequency, scrutiny and integrity of cyber reporting;
- strengthening the Trust's processes for managing AI-related risks;
- improving the Trust's approach to understanding and developing workforce digital skills;

- strengthening financial planning to clearly set out digital investment needs in the short, medium and long term; and
- improving the evaluation of digital solutions.

Key facts and figures

Of the Trust's workforce (approximately 1,200 employees), only 33 have completed the HEIW interactive self-evaluation tool as part of the Digital Capability Framework.

Since April 2024, the Trust have only had two cyber incidents; however, it has had no reportable incidents per the Network and Information Systems Regulations 2018.

In March 2023, the Trust were assessed at Stage 1 of the HIMSS EMRAM model, meaning core digital systems are in place. Strategic initiatives, including the implementation of electronic prescribing, are underway to advance this level.

The Trust has achieved accreditation under the Digital Inclusion Charter in recognition of its Digital Inclusion Plan.

From 2021-22 to 2024-25, the Trust invested approximately £19.4 million in Digital, Data and Insights revenue and £12.2 million in capital.

Between 2025-26 and 2028-29, the Trust has forecast total expenditure of circa £33 million on Digital, Data and Insights revenue and £6.4 million on capital.

Our findings

Strategy, Planning and Leadership

The Trust has a clear digital strategy, but better alignment with organisational plans and stronger Board profile is needed to fully support digital transformation

Digital strategy and plans

10 The Trust has a clear 10-year Digital Strategy, approved by its Board in 2023. The strategy is available on the Trust's website and is reviewed annually. The strategy is built around six main themes, and each theme has clear goals and actions that cover all parts of digital transformation.[1] This clear structure provides a strong foundation for the Trust's digital plans and shows it understands both the opportunities and challenges of digital.

11 The Digital Strategy is linked to the Trust's long-term strategy, Destination 2033. However, the Trust could better align the strategy to other organisational strategies, such as the People Strategy and Clinical Strategy, to maximise its impact. The strategy is appropriately aligned with national digital transformation priorities, including the Welsh Government's "Once for Wales" ambitions. The Trust has committed to adopting several national systems to support these goals, showing strong alignment with wider sector goals.

[1] The six themes are: Ensuring Our Foundations, Digital Inclusion, Insight-Driven Services, Safe and Secure Systems, A Digital Organisation, and Working in Partnership.

12 The Trust has set out a realistic and deliverable short to medium-term plan for digital transformation in its Integrated Medium Term Plan (IMTP) for 2023-26. These plans focus on modernising core systems, moving services to cloud platforms, and enhancing cyber security to reduce operational risk. However, the Trust's plan beyond 2026 is not clearly defined and costed.

13 The Digital Strategy is based on a realistic view of the Trust's current digital maturity, supported by a Healthcare Information and Management Systems Society (HIMSS), that led to the Trust being rated at Stage 1.[2] It was also developed with input from staff and service users through workshops and focus groups supported by Llais.[3] Although Board members reviewed draft versions of the strategy before formally approving it, involving them earlier in the development process would have enabled broader and more meaningful Board input and engagement.

Board ownership of digital transformation

14 The Board shows a reasonable understanding of, and support for the Digital Strategy. To strengthen awareness of digital risks, Board Development sessions on information governance and cyber security were delivered in April 2025. However, the Health Board recognises that more digital education and awareness-raising is needed to help Board members provide stronger challenge, scrutiny, and strategic leadership as the Trust continues its digital transformation journey.

[2] Healthcare Information and Management Systems Society (HIMSS) Electronic Medical Record Adoption Model (EMRAM) Stage 1 signifies that the Trust has installed core ancillary systems for lab, pharmacy, and radiology.

[3] Llais is the national citizens' voice body for health and social care in Wales.

15 The Trust does not have an Independent Member or Board-level Champion for Digital, which potentially reduces the profile of digital matters at Board level. However, the Executive Director of Strategic Transformation, Planning and Digital and the Chief Digital Officer attend relevant Board and committee meetings as required. The Trust is no longer represented on the All-Wales IM Digital Network, a role undertaken by the previous Vice Chair. This reduces opportunities to share learning, exchange good practice, and contribute to national digital discussions that could support the Trust's own digital transformation.

Roles, responsibilities and accountability

16 There is clear accountability within the Trust for delivering digital transformation, supported by well-defined senior roles. Executive responsibility sits with the Executive Director of Strategic Transformation, Planning and Digital. Operational delivery is overseen by the Chief Digital Officer, who is responsible for three core functions: Digital Delivery, Digital Programmes, and Data and Insights.

17 Progress on the Digital Strategy is regularly reported to the Executive Management Board (EMB), the Strategic Development Committee (SDC), and the Board. Updates are shared every two months with the SDC through highlight reports. These reports give a clear view of progress, risks, and key dependencies. The performance of the Trust's digital services on operational matters such as safety, experience, timeliness, and efficiency is monitored separately, with appropriate oversight provided by the Quality, Safety and Performance Committee (QSPC).

18 The Trust is currently reviewing its committee structure. Although we did not identify concerns with the existing separation of oversight, the revised arrangements may offer opportunities to consolidate digital oversight within a single committee, potentially enhancing its profile at Board level.

19 The Trust also has a Digital Programme Board (DPB) that supports delivery of the Digital Strategy. Project highlight reports from digital programmes are presented to the DPB for assurance, giving a clear view of progress and risks. However, there is scope to strengthen how planned business benefits are tracked and reported to enable the Trust to more effectively evaluate project success.

Identifying and managing risks

The Trust has a good awareness of its digital risks, but its management of them requires strengthening

Digital infrastructure risks

18 While the Digital Strategy recognises the need to keep technology up to date, it does not set out clear timelines, milestones, or costed plans for doing so. This potentially limits the strategy's usefulness as a tool for prioritisation and oversight. The Trust does, however, use an up-to-date inventory of digital services and equipment, supported by an automated asset-verification tool, to manage infrastructure lifecycles and identify obsolete components.

19 Whilst digital infrastructure risks feature in the Trust's Risk Register and are reviewed by the Board, greater assurances are required on how the Trust are managing and mitigating the risks. For example, the Trust's Risk Register highlights issues caused by old systems that require manual workarounds, such as errors in test results. While the Trust has put controls in place and is monitoring progress, some actions still lack clear deadlines, cost information, and measurable outcomes.

20 Major infrastructure requirements are taken forward through formal business cases which are generally well-structured. Although the examples we reviewed were based on several assumptions, such as capacity risks and financial uncertainties, the established governance arrangements ensured they were tested and scrutinised before reaching the Board for approval.

Cyber resilience

21 Cyber security is a core component of the Trust's Digital Strategy, which commits the organisation to protecting data, strengthening cyber resilience, and meeting national standards. The strategy is supported by a comprehensive Cyber Security Strategic Delivery Plan aligned to the National Cyber Security Centre's "10 Steps to Cyber Security", with actions scheduled through to 2027 covering governance, resilience, system monitoring, and awareness.

22 However, the Cyber Resilience Unit's (CRU) July 2025 review highlighted key gaps, including the absence of an Incident Response Plan and inconsistent use of cyber-checks during procurement. Although the Trust has experienced only two cyber incidents since April 2024, neither of which were notifiable to the CRU under the Network and Information Systems Regulations 2018, the fact that cyber incidents and alerts are only reported annually to the QSPC limits timely oversight and responsiveness to emerging threats.[4] Cyber security risks appear in the Trust Risk Register and Board Assurance Framework. However, more recently, the scoring of the risks has passed the threshold for explicit reporting at Trust Board level. An Internal Audit review of cyber security completed in 2025 provided 'Reasonable Assurance'. However, it noted weaknesses in how cyber risks are managed by the Trust.

23 The QSPC receives regular updates on cyber security performance, including training results, phishing-test outcomes, and progress against the NIS Cyber Assessment Framework (CAF). At present, the Trust presents its CAF position as a single compliance percentage. However, the CAF is designed to support structured discussion of cyber risks and organisational maturity rather than produce a simple compliance score. While it is positive that the Trust reports transparently on its current position, assurance would be strengthened by showing how many CAF principles and contributing outcomes have reached the required maturity level, supported by narrative explanation of remaining gaps and planned actions.

---

[4] The National and Information (NIS) Regulations 2018 aim to improve the cybersecurity and resilience of systems that provide essential services.

24 The Trust maintains important external relationships with the CRU, the National Cyber Security Centre, and Digital Health and Care Wales, drawing appropriately on their guidance, standards, and expertise. For example, the Trust is currently working with these partners to address weaknesses identified in the CRU review and strengthen delivery of its Cyber Security Strategic Delivery Plan. However, this reliance highlights the need for further investment in increasing the Trust's internal cyber security capacity and capability.

Artificial intelligence

27 The Trust is starting to develop a clear vision for how it wants to use Artificial Intelligence (AI) as part of its wider digital transformation. As a result, it is now reviewing its Digital Strategy to make its AI ambitions clearer and more specific.

28 It is also developing a separate AI strategy and recognises its success will rely on strong foundations. These include having a clear clinical operating model, reliable systems and processes, high-quality data, and well-defined use cases. However, the Trust does not yet have a full understanding of the level of resources needed to deliver its AI plans or how it will track and measure its impact.

29 Although AI is included in the Board Assurance Framework, the controls do not clearly match the AI-specific risks. Furthermore, the Board does not feel it receive enough assurance on how these risks are identified, managed, or reduced. While the Trust's existing policies and procedures for information governance and data protection provide some assurance, but they do not fully cover the ethical, legal and financial risks that come with AI technologies.

Digital skills

While the Trust is proactively developing digital skills across the workforce, it needs a more co-ordinated approach to identify a clear baseline of need

Assessing digital skills

30 The Trust does not yet have a full understanding of digital skills across its workforce. The Digital Strategy mentions using accredited audits to measure digital confidence, but there is currently no clear plan or method for doing this. Instead, the Trust has started using the Health, Education and Improvement Wales (HEIW) Digital Capability Framework. However, only 33 of around 1,200 staff have completed the self-evaluation so far. The tool seeks to assess basic IT skills and confidence and does not assess the wider skills that may be needed to support digital transformation. The Trust recognises that it needs to do more to promote uptake of the HEIW framework as well as assess the wider skills required for digital transformation. However, the Trust does conduct a digital training needs analysis for each of its programmes and ensures that these are completed as part of the go-live criteria.

Developing digital skills

31 The Trust is committed to developing a digitally skilled workforce. The Digital Strategy and People Strategy aims for staff to be confident using digital tools. Both strategies are aligned with national programmes and include short, medium, and long-term actions to improve digital skills. These include working with HEIW and the Intensive Learning Academy and building digital skills into transformation programmes. However, it is unclear whether responsibility for developing digital skills sits with the Digital Team or the Organisational Development and Workforce Team. This lack of clarity could potentially impede progress, lead to duplicated or uncoordinated work and effort, and make it harder for the Trust to build the skills needed to support its digital transformation ambitions.

32 The Trust has taken some steps to support digital skills across its workforce. It has launched a Digital Training Platform that gives staff access to training on key systems. Other resources include online courses, e-learning, and virtual workshops. Induction and tailored training programmes also help staff build the digital skills needed for their roles.

33 The Trust has also invested in professional development for the central digital team, including support for advanced qualifications, which shows commitment to keeping and developing specialist talent. Although the Trust has a well-established Digital Team, it continues to identify the recruitment and retention of skilled staff as a significant risk.

Collaboration and involvement

The Trust demonstrates a strong and proactive commitment to inclusive, user-centred digital transformation

Staff and service user involvement

34 The Trust's approach to involving staff and service users in digital design is positive but lacks the structure needed to ensure consistency and impact. The Trust involves staff and service users in designing and developing digital systems, with Business Analysts working closely with frontline teams to make sure new solutions meet operational needs. This approach is strengthened by active leadership from the Chief Clinical Information Officer and Chief Nursing Information Officer, which helps ensure clinical and user views shape digital transformation.

35 User involvement has helped improve digital services and inform decision-making. Initiatives such as the Digital Design Authority, training on user-centred service-design and the Digital Inclusion Plan show a strong focus on understanding what users need. Staff, volunteers, and service users have also helped shape projects such as the Digital Heroes network, the Digital Training Platform and improvements to the Digital Service Desk. Stakeholders also gave good feedback on the Electronic Prescribing and Medicines Administration (ePMA) business case because they were involved while it was being developed.

36 However, while some projects use agile methods and recognised service-design standards, the absence of a formal approach to involving staff and service users in digital design creates a risk of inconsistent, fragmented, and poorly co-ordinated engagement across programmes.

Reducing digital exclusion

37 The Trust has taken steps to reduce digital exclusion by appointing a dedicated lead and approving a detailed Digital Inclusion Plan for 2024-25. It is evidence-based, accredited under the Digital Inclusion Charter, and uses information from national surveys and policies.[5] While the plan is reviewed annually, there is no evidence that the Trust has prepared an updated plan for 2025-26.

[5] The Digital Inclusion Charter exists to support and champion organisations in Wales which are willing to promote basic digital skills and help people get online.

38 The plan for 2024-25 identifies which groups are most at risk of digital exclusion and considers wider challenges, such as the rising cost of living and the "digital inverse care law."[6] Although the Trust understands these issues well, the plan would be stronger if it included more specific and focused actions to measure progress. Furthermore, there is no evidence that the Board or its committees receive assurance on the delivery on the Digital Inclusion Plan. However, Trust business cases show that quality and equality impact assessments are completed to ensure that digital transformation is fair and accessible to everyone.

Partnership working

39 Working with national organisations is an important part of the Trust's Digital Strategy. The Board receives updates on how these partnerships are progressing through the SDC. The Trust also takes part in many forums such as executive meetings, national project groups, and the Director of Digital Peer Group.

40 The Trust works with organisations outside of NHS Wales to find new ways to innovate and keep up with changes in the digital world. This approach includes learning from private-sector organisations such as Amazon and AToS.[7] However, there is limited evidence within the reports to SDC to demonstrate the impact of these engagements to share learning.

[6] The Digital Inverse Care Law refers to a situation in which the people who most need new digital services are the ones most likely to be left behind because they lack the necessary digital skills and access.

[7] AToS is a global leader in digital transformation, specialising in IT services, consulting, cloud, cybersecurity, and high-performance computing.

41 The Trust also works closely with the public and third-sector, such as Digital Communities Wales, the Centre for Digital Public Services, Digital Health and Care Wales (DHCW), and HEIW. These partnerships have helped to develop staff skills to improve service design. For example, the Trust worked in collaboration with the Centre for Digital Public Services to run joint training courses on service design approaches to ensure that staff are equipped to design services that meet user needs and support consistent, high-quality digital transformation.

Using digital developments to support service transformation

The Trust is progressing digital solutions but needs to increase investment and strengthen evaluation to ensure digital priorities deliver intended outcomes

Investment in digital transformation

42 The Digital Strategy does not set out detailed short, medium, or long-term investment plans. Instead, the short and medium-term investment priorities are set out in the Trust's IMTP. However, the Trust has expressed concerns about whether it has enough resources to deliver all of its digital plans in the IMTP, partly due to the competing demand of balancing local priorities with national programmes. The Trust also recognises that it needs to improve its approach to evaluating the cost benefit of digital investment to strengthen its approach to financial planning and resource allocation.

43 **Exhibits 1 and 2** show that the Trust's overall digital investment has gradually increased to around £10 million a year, mainly due to rising revenue costs. Capital funding is much more unpredictable, with a noticeable drop in 2026-27 due to the significant increase in revenue expenditure associated with moving services to cloud platforms. While the rising investment shows commitment to digital modernisation, the imbalance between capital and revenue, along with uncertainty about long-term investment, creates risks for delivery of the Trust's digital ambitions.

Exhibit 1: Annual capital and revenue investment in digital (2021–22 to 2024–25)

Financial Year	Capital (£'000s)	Revenue (£'000s)
2021-22	£2,202	£3,998
2022-23	£3,825	£3,916
2023-24	£2,522	£5,089
2024-25	£3,656	£6,443

Exhibit 2: Planned levels of capital and revenue investment in digital (2025-26 to 2027–28)

Financial Year	Capital (£'000s)	Revenue (£'000s)
2025-26	£2,473	£8,160
2026-27	£722	£8,997
2027-28	£2,611	£8,107

Local and regional digital projects

44 The Trust is exploring advanced technologies to enhance and modernise its services. For example, clinicians are using AI in radiotherapy treatment planning to aid decision-making and improve patient outcomes. The Trust has also given Microsoft Copilot to over 200 staff to automate routine tasks, so they have more time to focus on important work. The Trust is also using robotic process automation in back-office areas like finance to reduce manual work and increase productivity.

45 Digital projects, whether regional or national, are managed through three main programmes – Velindre Futures, Welsh Blood Service Futures, and the new Velindre Cancer Centre. Overall prioritisation is handled by the DPB, which uses a MoSCoW approach to rank projects based on how much they could improve access, quality, efficiency, and productivity.[8] This gives the Trust a structured way to decide which projects matter most.

46 Recommended projects go to the EMB and SDC for review before being added to the IMTP. However, the Trust would benefit from clearer evidence on how these decisions maximise benefits and address organisational risk, to give greater confidence that resources are being used to the best effect.

47 All digital projects in the IMTP have clear timelines and milestones. Progress is monitored using highlight reports and dashboards with detailed performance measures. These reports show how digital investments improve care pathways and make services more efficient.

48 To support delivery, the Trust is continuously improving its processes and governance. It has recently set up a Change Advisory Board and a Digital Design Authority. These groups manage new requests and make sure digital products and services are introduced properly. They also help ensure changes and new initiatives are aligned to the Trust's strategic goals.

[8] The MoSCoW method is a technique for prioritising digital projects, where the acronym stands for ‘Must have’, ‘Should have’, ‘Could have’, and ‘Won’t have’.

Adopting national digital systems

49 The Trust has agreed to use several national systems to support national goals, such as the Radiology Informatics System, Laboratory Information Management System, and ePMA. Adopting the Electronic Health Record and National Data Repository are also important priorities. This shows that the Trust is well aligned with national digital priorities. However, it has expressed concerns around its limited resources and capacity to support delivery of national digital programmes and the associated impact on delivery of local digital projects. These challenges make it harder for the Trust to plan confidently and increases the risk of delays to its digital transformation.

Evaluating digital solutions

50 The Trust does not yet have a standard way of evaluating its digital solutions. Although it tries to identify benefits during the planning stage, the Trust could do more to track and measure these benefits throughout the whole project. Gaps in evaluation and assurance processes create risks that may stop the Trust from achieving the full benefits of digital transformation.

51 The Trust does not routinely measure how satisfied users are with its digital services, so it is hard to fully understand how digital projects affect everyday work and service quality. The IT service desk does meet its targets and has a high user-satisfaction score of 96%. But this mainly shows how staff feel about the support they receive at the time, rather than how they feel about the wider digital systems they use. As a result, the Trust does not have enough insight into how well new digital tools are being used, whether they improve work and outcomes, or where further improvements are needed across services.

Recommendations

52 The following table details the recommendations arising from our work.

R1 The Trust should strengthen its oversight and monitoring of digital infrastructure risks by introducing a more structured approach to tracking and reporting progress against mitigating actions (see **paragraph 20**).

R2 The Trust should improve cyber security oversight by:

- **R2.1** increasing the frequency and timeliness of reporting cyber incidents and alerts to the relevant committee;
- **R2.2** providing stronger scrutiny and oversight of cyber matters; and
- **R2.3** revising CAF compliance reporting (see **paragraphs 22 and 23**).

R3 The Trust should strengthen its arrangements for identifying and managing risks related to the organisation's use of Artificial Intelligence (see **paragraph 29**).

R4 The Trust should strengthen its approach to understanding and developing digital skills in the workforce by:

R4.1 increasing participation in the HEIW Digital Capability Framework self-assessment;
R4.2 creating a clear plan for measuring digital confidence and monitoring progress over time; and
R4.3 assessing the technical digital capabilities within the core digital team (see **paragraph 30**).

R5 The Trust should strengthen its digital investment planning by creating a comprehensive, phased financial plan that clearly sets out short, medium and long-term investment needs (see **paragraph 42**).

R6 The Trust should strengthen its approach to evaluating digital solutions by developing a standardised evaluation framework, strengthening benefit-tracking processes, and implementing routine user-satisfaction measurement (see **paragraphs 50 and 51**).

Appendices

1 Management Response

Ref	Recommendation	Commentary on planned actions	Completion date for planned actions	Responsible officer (title)
R1	The Trust should strengthen its oversight and monitoring of digital infrastructure risks by introducing a more structured approach to tracking and reporting progress against mitigating actions (see **paragraph 20**).	Infrastructure risks, such as those highlighted in the report, are managed through the Trust risk management approach. Given the NHS financial constraints, resolving infrastructure risks is an ongoing medium/long term activity. Capital resource is more generally available for these items in each Q4 and the Trust maintains a prioritised list of Digital capital investments available for this purpose. A major focus this year has been the movement from Windows 10 to Windows 11. A review of the Trust's Digital infrastructure risks will be conducted to ensure that action plans in mitigating actions are strengthened, including **timescales for delivery and** any cost implications. This will be reported to the Digital Programme Board.	July 2026	Chief Digital Officer

Ref	Recommendation	Commentary on planned actions	Completion date for planned actions	Responsible officer (title)
R2	The Trust should improve cyber security oversight by: **R2.1** increasing the frequency and timeliness of reporting cyber incidents and alerts to the relevant committee; **R2.2** providing stronger scrutiny and oversight of cyber matters; and **R2.3** revising CAF compliance reporting (see **paragraphs 22 and 23**).	**R2.1** Following Board review the QSPC have agreed to receive Cyber Security reports on a quarterly basis, rather than Annual basis. Overall committee structures are under review. **R2.2** Reporting on Cyber matters on a quarterly basis will allow for additional scrutiny and oversight. **R2.3** The overall CAF score is currently aggregated into one overall KPI of compliance presented in the Performance Management Framework (PMF). The underlying compliance levels in individual areas are available through CRU reporting and will be brought through more explicitly in the quarterly committee reporting. Where the aggregated KPI score is used we will be clear on the limitations of the approach.	R2.1 June 2026 R2.2 June 2026 R2.3 June 2026	Executive Director of Transformation, Planning and Digital Executive Director of Transformation, Planning and Digital Chief Digital Officer

Ref	Recommendation	Commentary on planned actions	Completion date for planned actions	Responsible officer (title)
R3	The Trust should strengthen its arrangements for identifying and managing risks related to the organisation's use of Artificial Intelligence (see **paragraph 29**).	Since the fieldwork for the Digital Transformation Audit, the Trust has approved the Trust's AI Policy, which includes the AI risk management. This was in development at the time of the audit. AI initiatives continue to be subject to the overall Risk Management policy for the Trust and the AI policy now provides clear guidance for how these risks are to be treated. A specific AI risk review will be conducted to assure the Board that AI risks are in line with the AI Policy.	March 2026 August 2026	Chief Digital Officer / SIRO Chief Digital Officer / SIRO
R4	The Trust should strengthen its approach to understanding and developing digital skills in the workforce by:	**R4.1** A communication plan for engagement with the DCF will be undertaken and presented to the Executive Management Board. This will be subsequently used for planning	September 2026	Chief Digital Officer

Ref	Recommendation	Commentary on planned actions	Completion date for planned actions	Responsible officer (title)
	R4.1 increasing participation in the HEIW Digital Capability Framework self-assessment; **R4.2** creating a clear plan for measuring digital confidence and monitoring progress over time; and **R4.3** assessing the technical digital capabilities within the core digital team (see **paragraph 30**).	service development using the finding through IMTP and short-term improvement initiatives. **R4.2** The Digital Inclusion Plan (which is the Trust mechanism for improving digital confidence and the backing for the Trust's Digital Inclusion Certification) will be reviewed/updated and presented to EMB/Board Committees. This will include an update on the measures to be used on Digital Confidence (eg HEIW Digital Capability Assessment). **R4.3** Since the fieldwork for the Digital Transformation Audit, the Trust commenced a Digital Diagnostic using an experienced external partner. Included in this is a review of the technical capabilities and capacity of the central Digital team. This will be reported to the EMB/SDC for approval.	October 2026 July 2026	Chief Digital Officer Chief Digital Officer

Ref	Recommendation	Commentary on planned actions	Completion date for planned actions	Responsible officer (title)
R5	The Trust should strengthen its digital investment planning by creating a comprehensive, phased financial plan that clearly sets out short, medium and long-term investment needs (see **paragraph 42**).	Since the fieldwork for the Digital Transformation Audit, the Trust has commenced a Digital Diagnostic using an experienced external partner. Included in this is a review are options for short, medium and long-term investment in the central Digital team to build the capability and capacity to meet the demands of the plan. The diagnostic will report the investment required. The Integrated Medium Term Plan (IMTP) sets out the Digital enablers required to meet the medium term plan for the Trust and the funding requirements. Digital transformation requirements will continue to be progressed through the WG Digital Priorities Investment Fund (DPIF) recognising that DPIF is over-subscribed so not all investment cases will be approved and the capital investment is only made available on a year-by-year basis.	July 2026 April 2026 for IMTP submission	Chief Digital Officer Executive Director of Transformation, Planning and Digital

Ref	Recommendation	Commentary on planned actions	Completion date for planned actions	Responsible officer (title)
		A review of the long-term digital investment will be conducted alongside the next review of the Trust's Digital strategy and will be reported to EMB/SDC	October 2026	Chief Digital Officer
R6	The Trust should strengthen its approach to evaluating digital solutions by developing a standardised evaluation framework, strengthening benefit-tracking processes, and implementing routine user-satisfaction measurement (see **paragraphs 50 and 51**).	The Trust is implementing an overall Portfolio approach, including the evaluation of benefits from Portfolio activities, mainly at the most strategic Tier 1 and 2 levels. Digital transformation is included in the scope of the portfolio.	March 2027	Director of Places, Partnerships and Portfolio
		The Trust contributes to the National Benefits Framework approach for Digital through the DHCW All Wales Benefits Group. Digital have now adopted the framework in our Digital Programmes (eg EPMA, WHAIS). Benefits realisation reviews and being conducted in line with the business case. These will be more explicitly reported to the Digital Programme Board. A repository for the	September 2026	Chief Digital Officer

Ref	Recommendation	Commentary on planned actions	Completion date for planned actions	Responsible officer (title)
		benefits and lessons learnt has now been created. The Trust uses the Halo ITSM for feedback and measurement of user satisfaction with Digital Services, which is mainly related to transactional interactions (digital incidents and requests) currently. This will be extended to include wider measurement of the overall Digital service for presentation through the Performance Management Framework.	September 2026	Chief Digital Officer

2 About our work

Scope of the audit

The goal of this audit is to find out if the Velindre University NHS Trust is using digital technology to support service modernisation and efficiency. This included the approach to strategy, leadership and skills development for digital transformation, and how risks around digital infrastructure, cyber resilience and artificial intelligence are being managed.

Audit questions and criteria

Questions

Our audit addressed the following questions:

- Does the Velindre University NHS Trust have a well-led and appropriately resourced approach to digital transformation?
- Is the Velindre University NHS Trust developing the digital skills, capacity, and capability of its workforce?
- Does the Velindre University NHS Trust have a clear plan for managing its cyber resilience arrangements and digital infrastructure and how they will need to change to support its digital transformation ambitions?
- Does the Velindre University NHS Trust engage effectively with staff, partners, patients / service users to deliver its digital transformation ambitions and minimise digital exclusion risks?
- Is the Velindre University NHS Trust actively utilising new digital technology and data solutions to enhance the accessibility, quality, efficiency, and productivity of its services?

Criteria

Our audit questions were shaped by:

- External reference input from the Welsh Government, all-Wales NHS Directors of Digital, and Digital Health & Care Wales.
- Relevant Welsh Government strategies and plans.
- Relevant NHS Digital Transformation review reports completed by the National Audit Office and House of Commons Health and Social Care Committee.
- NHS England Department of Health & Social Care: A plan for digital health and social care policy paper.
- NHS England Transformation Directorate: What good looks like framework.

Methods

We asked Velindre University NHS Trust to:

- complete a self-assessment to help us understand how the organisation is undertaking digital transformation; and
- give us facts and figures about its spending on digital technology, staff digital skills, cyber resilience, and how it involves people in digital transformation.

We reviewed a range of documents, including:

- Board and committee papers and minutes.
- Key governance documents, including Digital Highlight Reports and Digital Annual Reports.
- Key strategies and plans, including Digital Strategy, People Strategy, Trust Strategy and IMTP.
- Key risk management documents, including the Board Assurance Framework and Corporate Risk Register.
- Relevant policies and procedures.
- Reports prepared by other relevant external bodies.

We interviewed the following key stakeholders:

- Chief Executive Officer

- Chief Digital Officer
- Chief Operating Officer
- Executive Director of Strategic Transformation, Planning and Digital, and Deputy Chief Executive Officer
- Director of Finance

We observed Board meetings as well as meetings of the following committees:

- Quality, Safety and Performance Committee
- Strategic Development Committee

About us

The Auditor General for Wales is independent of the Welsh Government and the Senedd. The Auditor General's role is to examine and report on the accounts of the Welsh Government, the NHS in Wales and other related public bodies, together with those of councils and other local government bodies. The Auditor General also reports on these organisations' use of resources and suggests ways they can improve.

The Auditor General carries out his work with the help of staff and other resources from the Wales Audit Office, which is a body set up to support, advise and monitor the Auditor General's work.

Audit Wales is the umbrella term used for both the Auditor General for Wales and the Wales Audit Office. These are separate legal entities with the distinct roles outlined above. Audit Wales itself is not a legal entity.

Audit Wales

Tel: 029 2032 0500

Fax: 029 2032 0600

Textphone: 029 2032 0660

E-mail: info@audit.wales

Website: www.audit.wales

We welcome correspondence and telephone calls in Welsh and English.

Rydym yn croesawu gohebiaeth a galwadau ffôn yn Gymraeg a Saesneg.