Audit and Governance Committee meeting

Date: 16 June 2026 –10.00am to 1.00pm (09.45am start for committee and SMT)

Venue: HFEA Office, 2 Redman Place, London E20 1JQ

Agenda item	Time
1. Welcome, apologies, declarations of interest and Chairs activities	10.00am
2. Minutes of previous meeting (CS) For decision	10.05am
3. Action log (MA) For information	10.10am
4. Internal Audit • Results and annual opinion (AA) • Core documents 2026-27 (AA) For discussion	10.15am
5. Audit recommendations • Progress with current audit recommendations (non DSPT) (MA) • Progress with current DSPT audit recommendations (TS) For discussion	10.30am
6. Annual Report and accounts (including the annual governance statement (MA) For discussion	10.40am
7. External audit completion report (ND/DG) For information	10.55am
8. Risk Update • Strategic Risk Register for discussion (SQ) • Committee discussion on potential horizon scanning items/items to add to deep dive discussion list (CS)	11.15am
9. Digital projects • Phoenix Programme - for information (LR)	11.35am
10. Resilience, business continuity management & cyber security (verbal) (MC) For information	11.45am
11. Information assurance and security (SIRO report) (TS) For discussion	11.55pm
12. Bi-annual HR Report (YA) For information	12.05pm

13. Government Functional Standards (verbal report) (TS) For information	12.20pm
14. Estates (verbal report) (TS) For information	12.30pm
15. AGC forward plan (CS) For decision	12.35pm
16. Items for noting (MA) • Whistle blowing • Fraud • Gifts and hospitality • Contracts and Procurement For information	12.40pm
17. Any other business (CS)	12.45pm
18. Session for members and auditors only	12.50pm
19. Close	

Next Meeting: 13 October 2026 (virtual meeting)

Minutes of Audit and Governance Committee meeting 24 February 2026

Details about this paper

Area(s) of strategy this paper relates to:	Regulating a changing environment Supporting scientific and medical innovation
Meeting	Audit and Governance Committee
Agenda item	2
Meeting date	16 June 2026
Author	Alison Margrave, Board Governance Manager
Annex:	AGC minutes

Output from this paper

For information or decision?	For decision
Recommendation	Members are asked to confirm the minutes of the Audit and Governance Committee meeting held on 24 February 2026 as a true record of the meeting.
Resource implications	N/A
Implementation date	N/A
Communication(s)	N/A
Organisational risk	Low

Minutes of the Audit and Governance Committee meeting on 24 February 2026 held virtually

Members present	Catharine Seddon, Chair Alex Kafetz, Deputy Chair Tom Fowler Anne Marie Millar
External Advisers	Nick Doran, National Audit Office (NAO) – External Auditor Dean Gibbs (KPMG) – External Audit lead Esther Hearn (KPMG) – Engagement Manager Andrew Angeli, Head of Internal Audit GIAA
Observers	Rachel McBryde, Department of Health and Social Care (DHSC) Kirean Lawerance, Department of Health and Social Care (DHSC) Dina Halai, Head of Policy Kezia Quarrie-Jone, Communications Manager
Apologies	Shabbir Qureshi, Risk and Business Planning Manager
Staff in attendance	Peter Thompson, Chief Executive Tom Skrinar, Director of Finance, Planning and Technology Clare Ettinghausen, Director of Strategy and Corporate Affairs Rachel Cutting, Director of Compliance and Information Morounke Akingbola, Head of Finance Sophie Tuhey, Head of Planning and Governance Alison Margrave, Board Governance Manager Martin Cranefield, Head of IT (items 9, 10 and 11) Kevin Hudson, PRISM Programme Manager (item 9) Luke Reader, Phoenix Programme Manager (item 9)

1. Welcome, apologies, declaration of interest and Chair's activities

1.1. The Chair welcomed everyone to the meeting and extended a warm welcome to those observing the meeting.

1.2. Apologies for absence were received from Shabbir Qureshi.

1.3. The Chair asked for any declarations of interest, there were none declared.

1.4. The Chair informed the committee that together with the Chief Executive and Director of Finance, Planning and Technology she had met with Dave Willis from GIAA in December 2025. She had attended an Institute of Regulation roundtable on AI and reminded the committee that arising from the committee effectiveness review, membership of the Institute of Regulation had been purchased for herself and the Head of Planning and Governance to provide greater oversight of developments within regulation and regulated sectors.

2. Minutes of the previous meeting

2.1. The Chair introduced the minutes from the previous meeting held 3 December 2025 which had been circulated to the committee members.

2.2. The committee agreed the minutes of the meeting held on 3 December 2025 as a true record and could be signed by the Chair.

3. Action Log

3.1. The Head of Finance presented the paper and provided the committee with updates on the actions which were completed, as detailed in the paper, and therefore these actions can be closed and removed from the action log.

3.2. The Chair noted that the External Audit Lead had circulated that morning the notes from the de-brief meeting so action 6.13 from December 2025 meeting could be closed and removed from the action log.

3.3. The Chair proposed that action 12.13 from October 2025 meeting could be closed and removed from the action log as the counter-fraud action plan was being presented later to the committee.

3.4. The Chair informed the committee that nearly all the actions arising from the committee effectiveness review had been completed and therefore could be closed and removed from the action log. In terms of the outstanding action, the committee were informed that the Audit and Risk Chair of the Health Services Safety Investigation Body (HSSIB) would be observing the October virtual meeting and HFEA would be undertaking a reciprocal visit to HSSIB in December.

3.5. The Chief Executive updated the committee regarding action 12.6 from December 2025 and gave a rationale for having the CaFC/PRISM deep dive in October 2026 and patient's complaints in early 2027.

Decision

3.6. The committee noted the action log.

4. Internal audit update report

4.1. The Head of Internal Audit (GIAA) presented this item and informed the committee that GIAA had now delivered on 80% of the 2025-26 internal audit plan with a further 20% at fieldwork stage. He thanked the HFEA for their collaboration.

4.2. The shared service standard which relates to Customer Service Questionnaires (CSQs) is currently off track and he encouraged the HFEA to complete the CSQs as these allow GIAA to continuously improve the service it provides.

4.3. Reference was made to the final audit reports for Risk Management and Cash Management and Non-current Assets and the key emerging risks and themes arising from these.

4.4. In response to a question the Head of Finance clarified that the assets awaiting disposal identified in the Cash Management and Non-current Assets do not sit on the balance sheet and it will be an action for the IT team to arrange disposal. The Director of Finance, Planning and IT stated that this is also a requirement within the DSPT improvement plan.

4.5. A member commented that the working relationship between the HFEA and GIAA seems to have improved and recognition was given to the HFEA team.

4.6. The Chair asked whether the indicative moderate annual opinion rating given in December 2025 still held good and asked whether progress been made on the rating from the previous year. The

Head of Internal Audit responded that there had been considerable improvement in the implementation of recommendations.

4.7. The Head of Internal Audit presented the proposed internal audit plan for 2026/27. These proposals had been discussed with the HFEA's Senior Management Team and had taken into consideration the strategic risks and audit coverage of previous years. The proposal is that the audits will be completed within the first three quarters of the year.

4.8. He commented that GIAA's approach in 26-27 will continue to be agile and a review with Management will be undertaken during the year to ensure that audit activity remains focussed on the right areas for the latter half of the year.

4.9. The Chair stated that the inclusion of the longer-term view was a very helpful addition and asked that inspections, EDI and Performance Reporting be added to this longer-term view.

Decision

4.10. The committee noted the progress made in delivering the 2025-26 internal audit plan and formally ratified the 2026/27 audit plan.

5. Progress with current audit recommendations

5.1. The Chair introduced this agenda item and informed the committee that as at the previous meeting the committee would first consider non-Data Security and Protection Toolkit (DSPT) audit recommendations and then the DSPT audit recommendations.

Non-DSPT audit recommendations

5.2. The Head of Finance introduced the main paper and informed the committee that all the actions arising from the Public Bodies review and Cash Management audits have been completed.

5.3. There were five recommendations arising from the Risk Management Strategy, some of which will be addressed by the revised Risk Management Policy which is brought to this meeting for review and approval. None are overdue.

DSPT audit recommendations

5.4. The Director of Finance, Planning and Technology introduced the paper on DSPT recommendations and informed the committee that three actions had been completed and were signed off by GIAA in February 2026.

5.5. In response to a question, the Director of Finance, Planning and Technology referred to the planned improvement programme and the areas that this focuses on with the ambition to complete several outstanding recommendations by the Summer.

Decision

5.6. The committee noted the progress made in implementing audit recommendations.

6. External audit

6.1. The External Audit lead (KPMG) introduced the paper which set out the audit plan for 2025-26.

6.2. The committee were advised of the initial assessment of the significant risk of material misstatement and audit focus areas. Three areas of significant risk were identified as:

- the presumed risk of management override;
- accuracy of revenue recognised; and
- a small number of clinics that have not onboarded into PRISM

6.3. The committee were advised that the risk regarding the valuation of PRISM intangible assets had been reduced and was now classified as an area of focus.

6.4. The External Audit Lead stated that materiality has been determined as 2.5% of expenditure.

6.5. In response to a question regarding the proposed timeline for preparation of the accounts the External Audit Lead clarified that there would not be an interim audit visit, as previously agreed with management and this should be removed from the timeline. If there were any matters which needed to be brought to the committee's attention, they would be brought up through the appropriate channels outside committee meetings.

6.6. In response to a question, the External Audit Lead stated that it was anticipated that a draft Annual Report would be provided to Audit colleagues at the beginning of the final audit visit. The aim is to be able to lay the HFEA's accounts in Parliament before summer recess.

6.7. In response to a question regarding revenue recognition, the Director of Finance, Planning and Technology explained the role of PRISM and for those clinics who are not yet fully using the PRISM system the separate engagement of the Finance Team in liaising with those clinics.

6.8. The Chief Executive commented that the uncertainty with PRISM was reducing and there were only a very small number of clinics who were not fully utilising the system.

6.9. The External Audit Lead referred to the proposed audit fee and apologised that this had not been communicated in an optimal way to the HFEA. The HFEA's audit was considered complex and risky due to PRISM, a bespoke system with unique coding, which requires the use of IT specialists for the audit to provide a required level of assurance.

6.10. The External Audit Lead spoke of the full scope of work covered by the audit and the need to recover costs. This had been discussed with NAO over the past few years and the fee contained in the paper reflects all the work that is required by KPMG.

6.11. The committee expressed strong concern and disappointment over the large increase in audit fees and the way that this had been communicated to the HFEA. The committee stated that this cost increase will be difficult for the HFEA to absorb so late in the year.

6.12. A DHSC finance representative echoed the concern about the timing of the proposed fee increase with just one month left in this financial year. He asked for increased transparency around future fee setting and asked for the impact on end users to be considered.

6.13. The External Auditor agreed to provide further information to the Chief Executive and Director of Finance, Planning and Technology on how the proposed fee had been set and why it is so much higher than that of previous years.

Decision

6.14. The committee noted the proposed plan and timetable for the preparation of the 2025-26 financial statements audit.

Action

6.15. External Auditor agreed to provide further information on how the fee had been set and to explain why it is so much higher than that of previous years

7. Accounting policies

7.1. The Head of Finance introduced the paper and stated that the purpose is to advise members of the accounting policies adopted for the preparation of the accounts for the financial year 2025/26. The Annual Report and Accounts will be prepared in accordance with the Financial Reporting Manual, International Financial Reporting Standards as adapted for the public sector and Managing Public Money.

7.2. The Head of Finance explained the rationale for the proposal to leave the useful economic life (UEL) for depreciation of PRISM at 10 years for 2025/26 but with annual reviews. The External Audit Lead confirmed that they were comfortable with this proposal.

7.3. In response to a question, the Chief Executive and Director of Finance, Planning and Technology reminded members that PRISM was a database that held information and like any IT system would need maintenance and updating but there were no plans for a replacement database.

7.4. The External Audit Lead informed the meeting that IFRS 17 should also be considered to see whether this has any impact on the HFEA. The Head of Finance confirmed that IFRS 17 does not affect the HFEA and apologised for the omission of this from the paper.

Decision

7.5. The Committee noted the accounting policies applicable to financial years 2025/26 and agreed the recommendation to leave UEL of PRISM at 10 years for 2025/26 but with annual reviews.

8. Strategic risk

Risk Management Policy

8.1. The Director of Finance, Planning and Technology introduced the paper and explained that changes have been made to the Risk Management Policy to simplify and condense the language, and to respond to recommendations from the recent internal audit of the HFEA's approach to risk management.

8.2. The policy will be reviewed formally every two years or following significant changes to the HFEA's operating environment, in line with a new organisational strategy, or updates to the Orange Book or other government risk management policies.

8.3. The Chair referred to paragraph 3.4 of the Risk Management Policy and questioned whether the statement regarding the risk-adverse attitude should also include the impact of failure to innovate.

8.4. The committee were supportive of the revised Risk Management Policy.

Risk appetite statement

8.5. The Director of Finance, Planning and Technology drew the committee's attention to the risk appetite statement contained in Appendix 1 of the Risk Management Policy.

8.6. The risk appetite statement has been updated to show the risk appetite for each section in bold for clarity (for example, "Appetite: Low"), which members agreed is helpful.

8.7. Members suggested revising the risk appetite for "information, reputational and security" risks from "low" to "low to moderate," noting that the HFEA publishes information in various formats and referencing the Authority's public discussion in November 2025 regarding the CaFC publication. The Chief Executive responded that the HFEA's risk appetite varies by type of information and could be clarified within the risk appetite statement.

8.8. The Chair queried whether a "Stakeholders" heading could be added to the risk appetite statement. While this category is not included in the Orange Book, the Chair noted that the HFEA manages its stakeholder relationships effectively, with a clear purpose for engagement, and suggested this could be reflected in the statement.

8.9. The Director of Finance, Planning and Technology thanked the Committee for endorsing the Risk Management Policy and confirmed that the suggestions regarding the risk appetite statement would be considered.

Strategic Risk Register (SRR)

8.10. The Director of Finance, Planning and Technology introduced the Strategic Risk Register (SRR), noting that this was the closing SRR for 2025–26 and would be included in the Annual Report and Accounts.

8.11. It was noted that the Senior Management Team had reviewed the SRR and the amendments made were outlined, including reframing of the financial and information risks.

8.12. The Committee discussed the information risks and queried whether the likelihood rating of the risk as framed should be increased in light of the rise and easy availability of DNA testing. The Chief Executive responded that the likelihood rating remained low, with just over 20 incidences recorded from the thousands of applications processed by the HFEA. The Director of Strategy and Corporate Affairs added that, over time, the introduction of witnessing and strengthened digital records management, should further reduce the likelihood.

Decision

8.13. The Committee approved the revised Risk Management Policy and agreed to recommend the Risk Appetite Statement to the Authority, advising that the risk appetite for information, reputational and security risks be amended to "low to moderate" and that consideration be given to introducing a new "Stakeholders" risk category. Additionally, an undertaking was given to review the wording of the (first) information risk.

8.14. The committed noted the Strategic Risk Register.

Horizon Scanning

8.15. The Chair invited members to raise any items under Horizon Scanning.

8.16. A member asked whether the pace of restructuring at DHSC, and the associated risks, should be included in the Committee's horizon scanning.

8.17. The Chief Executive advised that the restructuring within DHSC is progressing and confirmed that the HFEA has received confirmation that we will remain within its current directorate. The principal risk identified was ensuring that the HFEA's voice continues to be heard within the Department.

8.18. A DHSC representative highlighted the positive engagement with the HFEA and strong links within the Department, noting that the restructure should be viewed as an opportunity as much as a risk, with potential for increased ministerial exposure.

8.19. A member questioned whether AI, and the opportunities and risks it presents, should be captured as part of horizon scanning.

8.20. The Chief Executive stated that the HFEA had a good sense of how AI is being used across the sector and referred to the paper which had gone to the Authority meeting on 19 November 2025. Examples of good practice within the regulatory field, such as Ofsted reports, were noted and will continue to be monitored. It was also noted that ensuring the HFEA's IT systems are on a modern platform will support the future use of AI opportunities.

8.21. The Chief Executive reminded the committee that he had previously undertaken to consider how best to capture AI risk/opportunity in the next iteration of the SRR and work is progressing on this.

8.22. A member raised the issue of unregulated services and a fragmented patient pathway and questioned whether this can be modelled. The Chief Executive responded that the HFEA does not have oversight of unlicensed entities and reminded the committee of the HFEA's proposals for law reform.

9. Digital projects

PRISM update

9.1. The PRISM Programme Manager provided a verbal update to the committee noting that a written report was presented to the Authority at its meeting held on 21 January 2026.

9.2. The PRISM Programme Manager reported that 84 clinics had signed off their data in December 2025, with only five clinics outstanding. Of these, they noted that the three clinic group that is headed by the Assisted Reproduction and Gynaecology Centre (ARGC) is focusing on updating data for one clinic (the ARGC itself), and whilst activity had increased since mid-December, it has tapered off over the past three weeks.

9.3. The PRISM Programme Manager noted that, historically, only 6% of users accessing CaFC view the detailed statistics. An exception is ARGC itself, where approximately 50% of users accessing ARGC pages use the detailed statistics.

9.4. The PRISM Programme Manager stated that the team had identified some interpretational anomalies in the detailed statistics. As a result, these were temporarily suspended but are expected to be republished by the end of February.

9.5. The PRISM Programme Manager informed the Committee that the Authority, at its January meeting, approved the timetable for the publication of CaFC data in 2026. Work will commence in early March, with a planned publication in Summer 2026. PRs of clinics will shortly be advised that there are no changes to the headline figures, and the timetable will be shared with them.

9.6. A member noted that, although the detailed data is accessed less frequently, it remains important to provide this level of detail.

9.7. The committee congratulated the team on the successful publication of CaFC.

Phoenix Programme

9.8. The Phoenix Programme Manager introduced the paper.

9.9. A member asked whether the risk identified in the paper regarding the completion of the Dynamics build could impact the proposed July launch date. The Phoenix Programme Manager responded that the launch date is currently unaffected, although there is a cost implication.

9.10. The Director of Finance, Planning and Technology informed the Committee that a meeting with Ceox is scheduled later this week, and any necessary updates will be provided to members outside the Committee meeting.

Decision

9.11. The committee noted the reports on PRISM and the Phoenix Programme.

10. Resilience, cyber security and business continuity

10.1. The Head of IT provided a verbal report to the committee.

10.2. The Head of IT referred to the four workstreams outlined in paragraph 7.2 of the Business Continuity deep dive paper. Workstream #1 commenced in January and has been completed. Workstream #2 is scheduled to start in early February, workstream #3 is expected to finish in the Summer with the implementation of SharePoint, and workstream #4 will begin in February, with the majority of activity taking place in March.

10.3. The Head of IT updated the committee on a back-up failure that occurred with Epicentre (a legacy system in the process of being replaced) last week, whilst all data is secure a working group consisting of Licensing, Compliance and IT staff had been established to consider what steps could be taken to mitigate future potential failures. The committee were appreciative of the update noting that the limitations of Epicentre had been dealt with well.

Decision

10.4. The committee noted the verbal report.

11. Deep Dive discussion – business continuity

11.1. The Head of Planning and Governance introduced the paper which provided a review of the HFEA's business continuity arrangements including the Business Continuity Policy (BCP), Critical Incident Response Plan (CIRP) and related processes.

11.2. The Head of Planning and Governance provided further information on the exercise conducted in Summer 2025, which tested both the BCP and CIRP. The exercise confirmed that the existing text alert system for reaching staff in an emergency was effective, all staff participated, and there was a good understanding of the HFEA's emergency management and business continuity plans. Several recommendations were made to further strengthen the plans and associated documentation, outlined in the paper.

11.3. It was noted that DHSC expects all organisations managing patient information, including its ALBs, to comply with the new Cyber Assessment Framework-aligned Data Security and Protection Toolkit. The Head of IT spoke to the HFEA's current cyber improvement plan.

11.4. The Head of Planning and Governance referred to the business continuity risk register and outlined the nine risks identified in this register. The committee were informed that this information will be held in the operational risk register.

11.5. A member asked whether "business as usual" activities, such as Licensing Committee and Statutory Approvals Committee meetings, had been assessed to identify those that must continue during a critical incident, due to potential impacts on patients.

11.6. The Head of Planning and Governance confirmed that this is captured in the Business Continuity Risk Register (HR2) and highlighted proposed mitigations, including the re-deployment of staff to maintain critical activities and supporting functions. The Director of Strategy and Corporate Affairs noted the distinction between critical operations and other activities, and agreed to work with the Head of Planning and Governance to formalise the prioritisation of licensing activity.

11.7. A member commented that the documents provided were very comprehensive and that the July 2025 exercise had been beneficial. They asked about engagement with DHSC and what support the Department could provide.

11.8. The Head of Planning and Governance responded that the SOP (Critical Incident Response Plan) outlines the steps for incident classification and when engagement with DHSC is required. The SOP will be reviewed quarterly to ensure contact information remains accurate.

11.9. A member highlighted that if traditional communication systems fail and information is exchanged via WhatsApp, it is important to preserve this information, citing the Covid Inquiry as a learning point. The Committee discussed that the same access rights would apply to information communicated through WhatsApp.

11.10. A member cautioned that many organisations do not follow up on actions arising from lessons learned exercises and urged the HFEA have processes to avoid this.

11.11. A member suggested that a role was missing regarding ownership of record-keeping and transparency. It was agreed that this would be addressed offline with the Head of Planning and Governance.

11.12. The Chair commented that, following the closure of the next critical incident, a deep dive including a lessons learned exercise should be presented to the Committee.

Decision

11.13. The committee thanked the team for an excellent deep dive paper. They endorsed the Business Continuity Policy, the SOP and the new critical incident risk register.

Action

11.14. Deep dive/lessons learned from the closure of the next critical incident to be added to the deep dive long-list.

12. Draft Annual Governance Statement

12.1. The Head of Finance introduced the paper which set out the scope of the 2025-26 Annual Governance Statement and proposed timetable for production.

12.2. The Head of Finance informed the committee that the first draft of the Annual Governance Statement would be circulated to members, outside committee, on 6 April and members were

asked to respond within one week of receipt. Prompt response from members will allow for the full Annual Governance Statement to be provided to KPMG alongside first draft of the accounts.

12.3. The Chair asked members to diarise time for the review of the draft Annual Governance Statement.

Decision

12.4. The committee noted the proposed scope of the 2025-26 Annual Governance Statement and the planned timetable for production.

Action

12.5. Committee members to respond to the draft Annual Governance Statement email within seven days of receipt.

13. Counter Fraud and anti-theft Policy and Counter Fraud Action Plan update

13.1. The Head of Finance introduced the Counter Fraud and Anti-Theft Policy and reminded the committee that they reviewed this policy in March 2025.

13.2. The Head of Finance spoke to the proposed changes to the policy and explained that this policy will be brought to committee every two years but will be reviewed annually. If there are any major changes in law these will be picked up during the review process and the policy will be updated and presented to the committee at its earliest meeting.

13.3. The Head of Finance spoke to the Fraud Action Plan that had been derived from the Fraud Risk Assessments that were shared with the committee at its October 2025 meeting.

13.4. The Head of Finance informed the committee that the plan is updated each quarter and is submitted for peer reviews. Feedback received from DHSC Anti-Fraud Unit (AFU) was highlighted in the paper.

13.5. The Head of Finance informed the committee that a review and tests of controls, identified in the Fraud Risk Assessment, is underway and the results will be shared with the committee in due course.

Decision

13.6. The committee agreed the revised Counter Fraud and anti-theft Policy and that it should be reviewed by the committee every two years.

13.7. The committee noted that Fraud Action Plan and the feedback received from DHSC AFU and the Fraud Risk Assessment.

Action

13.8. Head of Finance to update the Counter Fraud and Anti-Theft Policy.

14. Public Interest Disclosure (Whistleblowing) Policy

14.1. The Head of Finance introduced the Public Interest Disclosure (Whistleblowing) Policy and reminded the committee that they reviewed this policy in March 2025. Since then, two reviews

have been undertaken to ensure the policy is still fit for purpose. The proposed changes to the policy were highlighted.

14.2. In response to a question, the Head of Finance stated that the policy is available on the staff intranet and is part of the required mandatory reading for all new starters as part of their induction process.

14.3. In response to a question, the Chief Executive stated that there is no Freedom to Speak Up Guardian on the Authority. The Chair commented that the policy is clear that people can approach her as Chair of the Audit and Governance Committee, and she believed that this was sufficient.

14.4. A member noted that paragraph 8.11 should read "Audit and Governance Committee Member" rather than "Audit Committee Member".

Decision

14.5. The committee agreed the revised Public Interest Disclosure ("Whistleblowing") Policy and that it should be reviewed by the committee every two years.

Action

14.6. Head of Finance to update the Public Interest Disclosure ("Whistleblowing") Policy.

15. AGC Forward Plan

15.1. The Head of Finance introduced the forward plan.

15.2. The Board Governance Manager informed the committee that the private meeting for committee members and the Senior Management Team had been scheduled for October 2026 and questioned whether this should be moved to an in-person meeting rather than a virtual meeting.

Decision

15.3. The committee agreed that the meeting with members of the Senior Management Team should be moved to immediately before the in-person meeting in June 2026.

15.4. The committee agreed that the deep dive on CaFC/PRISM should come to the October 2026 meeting and the deep dive on patients' complaints about licensed clinics should come to the February 2027 meeting.

Action

15.5. The Board Governance Manager to update the forward plan.

16. Items for noting

16.1. Whistleblowing

- Members were advised that there were no whistle-blowing incidents.

16.2. Fraud

- Members were advised that there were no fraud incidents.

16.3. Gifts and Hospitality

- The Head of Finance introduced the paper which was noted the committee.

16.4. Contracts and Procurement

- Members were advised that there was nothing to report.

17. Any other business

17.1. Committee members and observers reviewed the meeting noting the large number of items that had been considered, time management skills and efficient chairing.

17.2. The Chair reminded the committee of the schedule of meetings for the year being 16 June in person, 13 October virtual and 2 December in person and including training. The private session will start at 09.45am on 16 June and the main meeting will commence at 10am.

17.3. There being no further business the Chair closed the meeting and thanked all for their contributions.

Chair's signature

I confirm this is a true and accurate record of the meeting.

Signature

Chair: Catharine Seddon

Date: 16 June 2026

AGC Action Log

Details about this paper

Area(s) of strategy this paper relates to:	Regulating a changing environment /Supporting scientific and medical innovation
Meeting:	Audit and Governance Committee
Agenda item:	3
Meeting date:	16 June 2026
Author:	Morounke Akingbola, Head of Finance
Annexes	

Output from this paper

For information or decision?	For discussion
Recommendation:	To note and comment on the updates shown for each item.
Resource implications:	To be updated and reviewed at each AGC meeting
Implementation date:	2026/27 business year
Communication(s):	
Organisational risk:	Medium

Date and item	Action	Responsibility	Due date	Revised due date	Progress to date
17 June 2025 Item 12.13	Future SIRO reports to include information on structure policy for SharePoint	Director of Finance, Planning and Technology	June 2026		The Director of Finance, Planning and Technology will incorporate this into the 2026 SIRO Report. Please see agenda item 11. This action is complete and can be removed.
24 February 2026 Item 6.15	External Auditor agreed to provide further information on how the fee was set and why it is so much higher than previous years	External Auditor			Information provided via email. This action is complete and can be removed.
24 February 2026 Item 11.14	Deep dive/lessons learned from the closure of the next critical incident to be added to the deep dive long-list.	Board Governance Manager	June 2026		Item added to AGC forward plan. This action is complete and can be removed.
24 February 2026 Item 12.5	Committee members to respond to the draft Annual Governance Statement email within seven days of receipt.	AGC members	April 2026		The draft Annual Governance Statement was emailed to members on 6 April. AGC members and comments have been incorporated into the document found at agenda item 6. This action is complete and can be removed.
24 February 2026 Item 13.8	Head of Finance to update the Counter Fraud and Anti-Theft Policy	Head of Finance	May 2026		The Counter Fraud policy was updated after the February meeting and shared on the HFEA intranet. This action is complete and can be removed.
24 February 2026 Item 14.6	Head of Finance to update the Public Interest Disclosure (“Whistleblowing”) Policy.	Head of Finance	May 2026		The Whistleblowing policy was updated after the February meeting and shared on the HFEA intranet. This action is complete and can be removed.

Date and item	Action	Responsibility	Due date	Revised due date	Progress to date
24 February 2026 Item 15.5	Board Governance Manager to update the forward plan.	Board Governance Manager	April 2026		AGC forward plan updated. This action is complete and can be removed.

Phoenix Programme Update (from 5th Feb to 1st June 2026)

Details about this paper

Area(s) of strategy this paper relates to:	Regulating a changing environment
Meeting:	Audit and Governance Committee (AGC)
Agenda item:	9
Meeting date:	16th June 2026
Author:	Luke Reader, IT Project Manager
Annexes	3

Output from this paper

For information or decision?	For information
Recommendation:	The AGC is invited to note this report
Resource implications:	Over budget
Implementation date:	July 2026
Communication(s):	This information will be published on our website.
Organisational risk:	Medium

1. Progress Update

1.1. The Phoenix Programme (see *Annex A* for background and an overview of benefits) milestone dates are:

Milestone	Baseline Date	Projected Date	Actual Date
Discovery Complete	End-Mar-25	04/04/2025	11/04/2025
Design Complete	April-25	April-25	29/04/2025
Development & Testing	**Dec-25**	**Jun-26**	
Dynamics	**Feb-26**	**Jun-26**	
HFEA Portal Forms	**Dec-25**	**May-26**	May 2026
Content Manager Migration	**May-26**	**Jun-26**	
Go-Live	**Jun-26**	**Jul-26**	

1.2. Further details on the current timeline are provided in *Annex C*.

1.3. At the time of writing the launch dates are **at risk**.

1.4. Firstly, the **Content Manager** migration to **SharePoint** may need to complete in **July** rather than **June**. A replanning exercise in the first week of June will determine this.

1.5. The primary cause is that the Proof-of-Concept upload has shown that extract rates of data from Content Manager are so slow (about 1.5 Gig per hour) that it will take 600 hours to extract it all.

1.6. The replanning is considering the option to extract from two copies of CM in parallel in an attempt to double throughput.

1.7. Other factors in the delay have been in the pressures on the HFEA Infrastructure staffing team, which is both under-resourced (hiring is in progress) and has had to contend with Audits and with recent Website issues.

1.8. On the positive side, all planned SharePoint testing has now completed satisfactorily. All the staff training materials have been produced, with the first wave of those already published to all HFEA staff.

1.9. Secondly, the **Epicentre** migration to **Dynamics** may need to move back from **July**, potentially to **August**. Checkpoints in the first half of June will determine this.

1.10. The primary cause is that while there is noteworthy progress on the final build (of the Inspections functionality) and on resolving testing issues, there is likely to be still too much outstanding work needed to launch safely in July.

1.11. *Annex B* shows that most areas of functionality are at **70%-75% readiness to launch.** Equally, full end-to-end testing is now due to start in the second half of June, and experience tells us this exercise normally uncovers new issues.

1.12. The HFEA management and Martin Cranefield as the Product Owner are aligned that 'minor issues' that can initially be lived with should not delay the Dynamics launch. But our commitment to launching a system that is fit for purpose remains.

1.13. There is also a benefit to having the Dynamics launch scheduled for a month after the SharePoint launch, in terms of organisational change management and the ability of the project team to support the staff through both sets of changes.

1.14. A Change Request (CR) was approved back in March, after the last AGC Update. That CR was for additional Ceox development resourcing in May/June to support the intended July launch. It took the project costs to the level highlighted here (we had originally assumed a total cost, including VAT and 10% contingency, of £769k in January 2025, therefore we are currently around 24% higher than expected):

Phoenix Programme Costs	*Excl. VAT*	*Inc. VAT*
Programme Delivery Original Baseline	**£548,297**	**£657,956**
Net cost of changes identified in Discovery Phase	£38,650	£46,380
Programme Delivery Re-baseline *(June 2025)*	**£586,947**	**£704,336**
Cost of two approved CRs and extension of BA	£57,490	£68,988
Programme Delivery Re-Baseline *(Dec 2025)*	**£644,437**	**£773,324**
Approved CR for extended Dynamics build time	£118,503	£142,204
Programme Delivery Current Baseline *(Mar 2026)*	**£762,940**	**£915,528**
Cost of 1st 12 months support post-Delivery	£33,986	£40,783
Programme Delivery Baseline Costs with Support	**£796,926**	**£956,311**

1.15. If the Dynamics launch is moved back from July a further Change Request will be required.

2. Risks

2.1. The top risk stated in the previous AGC Update which has since been closed was (though a risk with a similar impact has now replaced it):

Ref	Title	Impact	Urgency	Description	Direction of Travel
R0056	**Dynamics Development effort**	1 - High	2 - Medium	Ceox have flagged a risk that the completion of the Dynamics build, including fixing all bugs and small changes identified, may require more time and resource than planned.	27th Mar – formal letter received from CEOX. Cost Forecast rebaselined. Risk closed. 2nd Mar - feedback is a new plan, still with a July launch but at a bit more risk due to testing/prep needed in June. Costs for FY26/27 increased by £118k (or £142k with VAT). Presented to Programme Board, discussed with SMT. 27th Jan 2026 - Ceox took an action at Programme Board to revert with options. None of these can involve additional spend this financial year. Likely they will involve more spend next year, and there may be pressure on the July launch date.

2.2. The top risks currently identified are:

Ref	Title	Impact	Urgency	Description	Direction of Travel
R0058	**Risk of testing-fix-retest cycles overrunning**	1 - High	1 - High	Following the rebaseline, there is no slack remaining between build->test->launch of the Dynamics system. So depending on the fit and quality of the final Dynamics build, there is a risk of testing overrunning and forcing the launch date to move back.	25th May: Testing is running smoothly in some areas, but is identifying further requirements to build or fixes needed in others. Checkpoints have been set in early June to determine whether we can still aim to launch in July or not. The overall per-month cost of slipping has been discussed with SMT. 15th Apr: new approach agreed for issue not blocking E2E testing but needed for live. 30th March - Risk raised. UAT and Integrations testing already in progress. Cannot start the End2End testing until Inspections is built, and Dynamics is linked to SharePoint.
R0060	**SharePoint data migration duration**	1 - High	1 - High	The PoC suggests 600 hours of downloads from CM will be needed. This would be 20 hours/day for 30 days which exceeds the current 4-week plan.	Ceox to look at the PoC findings, and at the possibility of running downloads from two CM instances in parallel. A decision day of Weds 3rd June has been set to decide on a new SharePoint migration plan, which will then show us whether the launch needs to move to July.

R0006	**Staff Engagement**	1 - High	2 - Medium	End-user engagement is vital both for designing fit-for-purpose systems and to ensure they are used willingly and as designed.	27th May – all SharePoint training materials complete. Briefing to HFEA 'Peer Sharing' meeting given. 3rd Feb 2026 - the draft SharePoint Staff Training plan was outlined to all staff at CEO-hosted weekly Teams call. 19th Dec - Phoenix briefing at All Staff Day included an exercise to gather staff sentiment in terms of both their 'Hopes' for Phoenix and their 'Concerns' as it might relate to their own work.

3. Conclusion

3.1. The core reasons for doing the Phoenix Programme remain valid. Epicentre is now running on an unsupported platform, and Content Manager is in 'extended support' which will itself end at some point.

3.2. Progress on build/test/migration/training has continued. User feedback on both new systems is consistently supportive of the view that they will be useful and usable once specific identified issues have been addressed.

3.3. The risks to timescales will be crystallised in June, and a Change Request raised if needed.

3.4. Senior HFEA management support remains with the Programme and the need to launch Phoenix successfully, and as soon as it is safe to do so.

3.5. The supplier relationship remains positive.

3.6. So, we are proceeding with the Phoenix Programme, with a potential replan in June if the checkpoints determine that is required. If this is the case, we will update AGC verbally on 16 June.

4. Recommendations for the AGC

4.1. The AGC to note this progress update for the Phoenix Programme.

Annex A – Background and Benefits

Background

- The HFEA has a core set of operational systems that it relies on to deliver its business that have reached, and in some cases, surpassed their useful lives, with one key system no longer running on a supported operating system nor receiving security updates. The risk of system failure has at times been significant. Furthermore, the systems no longer represent an efficient or effective tool for staff and user-experience is poor.
- The HFEA began scoping a replacement and improvement programme in the summer of 2023, looking at the following systems:
- The **Epicentre** system manages key processes such as scheduling inspections, writing inspection reports, managing licence applications, complaints, and incidents, etc., as well as issuing licences. The system was created internally over 15 years ago and is no longer supported. Its failure would be highly disruptive for the HFEA and would effectively prevent us from managing inspections or issuing licenses.
- The HFEA's **Clinic Portal** is the external web interface used by our regulated clinics, who use it to submit critical information to the HFEA such as licence applications. It is no longer delivering the service we require and suffers from significant performance issues.
- **Content Manager** is a now-outdated document management system that no longer meets our needs in a modern way and restricts our ability to maximise the value of the information that we hold.

Intended Benefits

The over-riding aim of the Phoenix programme is to replace our aging systems with modern, cloud-based solutions that will also provide us with options to innovate more easily, for example through use of AI, by having a much more effective and accessible structure for our data. The main benefits are:

- **System stability and resilience** – achieved by hosting the systems on industry-standard platforms;
- **Improved efficiency of staff processes** – through having key data in one system, and improvements such as automation of some of the Inspectors' tasks;
- **Clinic staff experience improvements** – new Clinic Portal won't crash and will be easier to use, resulting in fewer queries back to the HFEA;
- **Better data-management** – will support stronger reporting and responses to queries, FOIs, legal cases, etc, (including potentially through AI-based apps).

Annex B – Deliver phase

- The purpose of the **Deliver** phase is to turn the requirements (**User Stories**) into a working solution.
- The programme is working in 2-week iterations (**Sprints**) using the Scrum methodology including end-of-Sprint **demonstrations** to gain regular feedback.
- Built functionality is tested by Ceox, and then by HFEA staff in User Acceptance Testing (UAT).
- The programme is running three streams of **delivery** in parallel:

1. **Content Manager to SharePoint migration** – all planned build and test work has completed. Attention is now focussed on creating the new Production SharePoint environment and migrating over the Content Manager data.

2. **Clinic Portal** – all the Portal Forms have been built, 26 are signed off, with the final 3 requiring fixes before signoff. The rest of the Portal site is also largely built, as shown here:

Portal Forms

	Count	*%age*
in Requirements	0	0%
in Build	0	0%
in Ceox testing	0	0%
in User testing	3	10%
ready for Launch	26	90%
Total	**29**	**100%**

Static Web Portal User Stories

	Count	*%age*
in Requirements	9	6%
in Build	12	7%
in Ceox testing	24	15%
in User testing	6	4%
ready for Launch	112	69%
Total	**163**	**100%**

3. **Dynamics Build** (replacing Epicentre) – all areas have been built barring Inspections which is close to being done. User Testing is going on for all built areas in parallel. A day of onsite end-to-end testing involvement most HFEA user teams is scheduled for 23rd June.

   The position in terms of readiness-to-launch is shown here:

BSIS User Stories

	Count	*%age*
in Requirements	2	4%
in Build	7	13%
in Ceox testing	4	8%
in User testing	3	6%
ready for Launch	36	69%
Total	**52**	**100%**

Clinical Governance User Stories

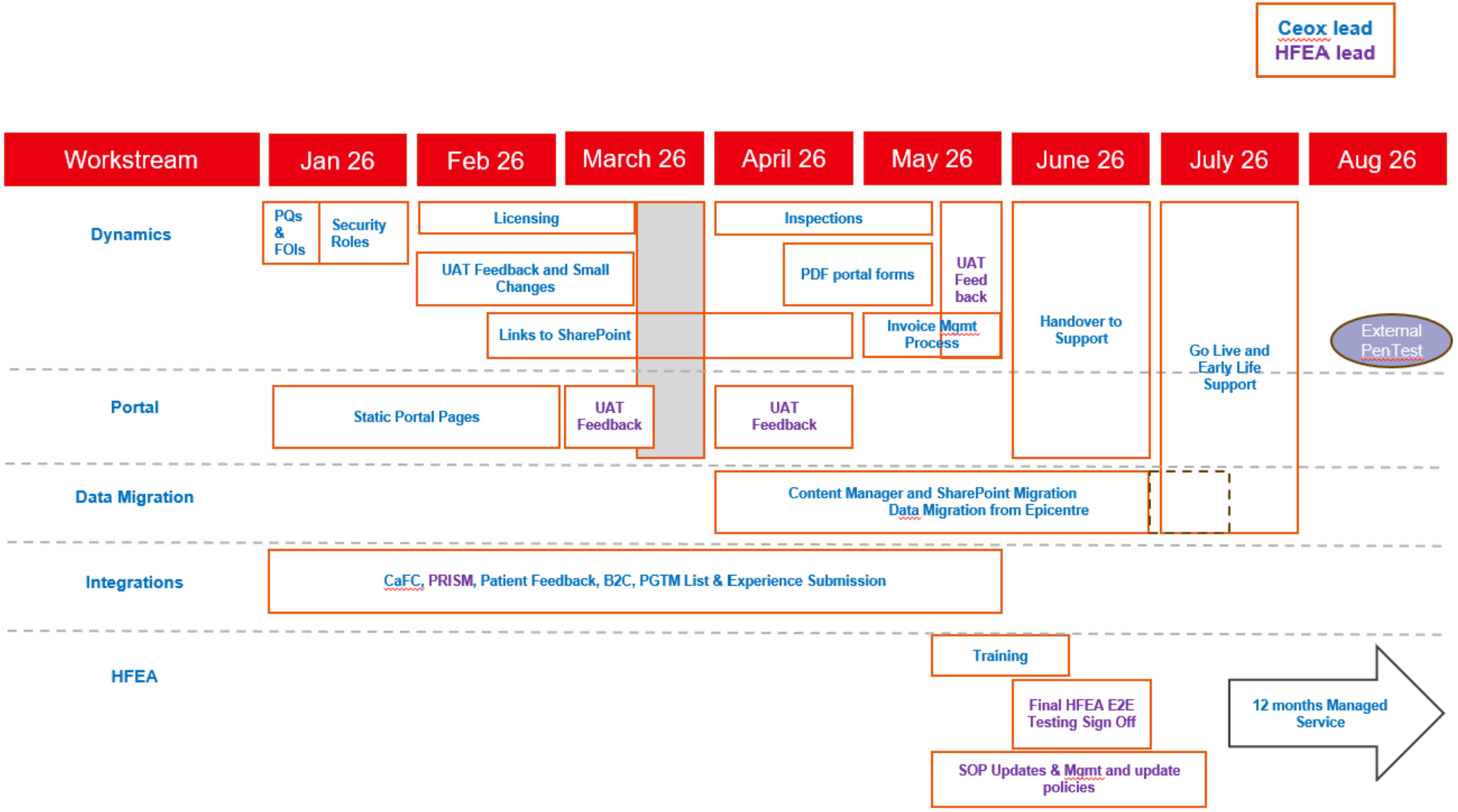
	Count	*%age*
in Requirements	2	4%
in Build	4	8%
in Ceox testing	4	8%
in User testing	4	8%
ready for Launch	37	73%
Total	**51**	**100%**

Licensing User Stories		
	Count	*%age*
in Requirements	5	6%
in Build	19	24%
in Ceox testing	6	8%
in User testing	10	13%
ready for Launch	38	49%
Total	**78**	**100%**

Inspections User Stories		
	Count	*%age*
in Requirements	7	17%
in Build	14	34%
in Ceox testing	18	44%
in User testing	2	5%
ready for Launch	0	0%
Total	**41**	**100%**

Comms & Policy User Stories		
	Count	*%age*
in Requirements	0	0%
in Build	3	4%
in Ceox testing	8	11%
in User testing	6	8%
ready for Launch	54	76%
Total	**71**	**100%**

Annex C - Current Phoenix Programme Timeline



SIRO Report 2025/26

Details about this paper

Area(s) of strategy this paper relates to:	Regulating a changing environment / Supporting scientific and medical innovation
Meeting:	Audit and Governance Committee
Agenda item:	11
Meeting date:	16 June 2026
Author:	Tom Skrinar, Director of Finance, Planning and Technology
Annex:	• Annex A: Information Governance and Cyber Security Steering Group - Terms of Reference • Annex B: Assessment of the HFEA's compliance with the mandatory requirements set out in the 10 National Data Guardian (NDG) standards for data security

Output from this paper

For information or decision?	For information
Recommendation:	N/A
Resource implications:	N/A
Implementation date:	N/A
Communication(s):	N/A
Organisational risk:	Medium

1. Purpose

1. The Senior Information Risk Officer (SIRO) holds responsibility for managing the strategic information risks that may impact on our ability to meet our corporate objectives, providing oversight and assurance to the Executive and Authority of the HFEA. It is a Cabinet Office (CO) requirement that Boards receive regular assurance about information risk management. This provides for good governance, ensures that the Board is involved in information assurance and forms part of the consideration of the Annual Governance Statement (AGS).
2. This is my annual report to the Accounting Officer and AGC, providing an overview of the key information and data governance activities and performance for the 2025/26 financial year. In addition, it aims to provide assurance to the Audit and Governance Committee that the HFEA remains compliant with its statutory and regulatory obligations.

2. Background and Governance

3. The HFEA routinely assesses the risks to information management across the organisation, through its assessment of the risk of data loss, cyber security and the inclusion of guidance on creating and managing records throughout its Policies and Standard Operating Procedures (SOPs).
4. The HFEA has historically held and processed personal data and records and maintained robust controls and security protocols around all data relating to fertility treatments, which it is required to hold under the HFE Act. In recent years we have also responded to changes in legislation relating to the broader personal data we hold in relation to our staff, clinic staff and members of the public who may have contacted us. We continually review the effectiveness of our policies and SOPs to ensure we comply with relevant legislation, including the UK General Data Protection Regulation and the Data Protection Act 2018.
5. This work is overseen by the HFEA's Information Governance Manager, who administers and reports to the Information Governance and Cyber Steering Group, which was newly created in 20206/27 after the agreement of the HFEA's information governance and security risk management HFEA position paper at AGC in June 2025 (see Annex A for the Terms of Reference). This group is chaired by me as SIRO and attendees include the HFEA's Data Protection Officer, the Director for Compliance and Information, The Head of Information (and Caldicott Guardian) and the Head of IT. This Group considers information and cyber risk management and data protection issues as well as ensuring that the HFEA has an up to date understanding of relevant regulatory requirements.
6. Information Governance and Security risks are discussed as part of the HFEA's broader approach to Strategic and Operational Risk Management at CMG at an Operational level and at AGC at a Strategic level, as well as periodically with the full Authority. AGC is also provided with regular updates on Information Governance and Security as well as progress in meeting DHSC and broader government expectations,

such as the Cyber Assessment Framework (CAF) aligned Data Security and Protection Toolkit (DSPT).

3. Resourcing and systems

7. The small size of the HFEA and limited dedicated resource has made it difficult for us to continuously adjust our response to the growing scale and range of risk, as expected by DSPT and other cross-government information risk initiatives. The HFEA's approach to managing information risks, including information security risks, is currently under development as outlined in last year's position statement, supported by some external consultancy advice procured using the NHS Cyber Investment Fund. Further work is still required, but there are a number of key changes that have happened in 2025/26 that support our approach.

Information Governance

8. Information Governance (IG) can be a resource intensive area of work and the HFEA manages a relatively high volume of Subject Access Requests, Freedom of Information requests, as well as having to respond to data breaches when they happen (see the section below on activity), provide training and awareness for HFEA staff and support projects to produce robust Data Protection Impact Assessments (DPIAs).

9. The IG team went through a number of changes in 2025/26 to increase capability and capacity in the team. There was also some structural change, with the team moving from the Compliance and Information Directorate to the Finance, Planning and Governance Directorate, with some additional roles taken on (in particular oversight of FOI responses from summer 2026). As part of this change, we created a new permanent role (through a re-prioritisation of internal posts) to support the IG team, in particular with oversight of the IG and Cyber Steering Group and the DSPT Improvement Plan.

10. In recognition of growing pressures on our IG manager to manage business as usual tasks as well as supporting SharePoint migration, we also recruited additional fixed term support in 2025 to allow the IG manager to focus on strategic improvements and on maximizing the benefits of our new support systems (Privacy Engine, an IG management system, as well as Purview, which will provide records management functionality for SharePoint).

11. PrivacyEngine is a data privacy management platform that we have been implementing through 2025/26 that helps identify, manage and mitigate data protection risks, while supporting GDPR compliance through automated reporting workflows, incident reporting, case management and training. It supports the handling of key IG activities such as data access requests, data breaches, vendor management for supply chain assurance, Data Protection Impact Assessments (DPIA), and Records of Processing Activities (RoPA) for comprehensive data audits. Implementation will continue in 2026/27, in particular looking at training and risk management.

12. A further key area of strategic improvement in 2026/27 will be through the Phoenix programme, in particular the replacement of Content Manager (CM), our document management system, with SharePoint. SharePoint will provide a number of benefits, in particular allowing us to improve our data management, which will facilitate quicker and more effective reporting and responses to queries, FOIs, legal cases, etc. It should also provide further options to automate records management, including document retention rules and keeping policies and SOPs up to date.

13. In order to ensure that we can make the most of SharePoint whilst remaining compliant with regulations, the IG team have commenced a record management project, agreed at CMG in April, that will establish the business-led rules, classifications, and lifecycle requirements that define how information and records should be managed across the organisation. This will be supported by Purview. We expect this project to run until the end of this financial year and will in particular revise our records management SOPs and policies, create a new Information Asset Register and embed an effective and pragmatic records management culture across the HFEA, using our new systems and supported by training and the engagement of data champions (who are responsible for information oversight within their teams).

IT and cyber

14. It has been clear for some time that the HFEA's IT resource has been insufficient to meet growing demand from both organisational use of changing technology and responding to the growing risk of cyber-attacks. An IT plan was agreed with SMT in January that aims to increase internal HFEA IT resource to ensure we are able to manage a range of technical tasks and allow the Head of IT to have a more strategic focus.

15. The cost of this additional resource will be more than covered by ending two external IT support contracts that were no longer providing value for money or providing us with the resource that we really need – proactive resource that can be delegated full responsibility for overseeing tasks or taking forward projects. The insourcing proposal has been agreed with DHSC and we commenced recruitment for a senior infrastructure engineer in May.

16. We procured cyber consultancy support at the beginning of the calendar year and a number of tasks and projects have been delivered by our partner Saepio, with the rest nearing completion. The work commenced with a cyber resilience assessment and a proposed Target Operating Model (TOM) and has provided a range of support to ensure we can set up SharePoint in a secure and well-managed way. Final work includes a focused review of our policies and SOPs, a review of our security risk management approach and review of our incident response approach, including a planned table-top exercise.

17. We will address the output of this work in detail once Pheonix has gone live and we have recruited additional resource. The TOM in particular provides a clear blueprint for how our cyber posture could be better developed, but will require some work to consider how best to fit it to our changing resources and requirements, as well as an increasingly active position from DHSC/NHSE cyber leads. It also provides

suggestions for specific external support, including monitoring services or a virtual Chief Information Security Officer (CISO).

18. We have been engaging with DHSC and NHSE to a much greater extent this calendar year, driven by a stronger focus from the Department on working with ALBs to find shared service improvements and efficiencies. This includes cyber, and we have been engaging with the Department on the Cyber Accelerator, including meetings with Phil Huggins and the NHS Cyber Security Operations Centre. There are a number of support options currently available, particularly through the CSOC, as well as a shared service-type support model for cyber under development within the Department. We will continue engaging on this and hope to cover some of the requirements in our TOM through these support offers where appropriate.

4. The Cyber Assessment Framework

19. The DSPT is an evaluation of an organisation's ability to manage cyber and information security risk – a requirement for NHS bodies and the Department of Health and Social Care (DHSC) arm's length bodies (ALBs). It is aligned with the Cyber Assessment Framework, which is the National Cyber Security Centre's (NCSC) standard. It includes 47 expected outcomes across 5 areas, with an expectation that outcomes are achieved or partially achieved each year, with expectations increasing each year up to 2030.

20. Our 2025 DSPT submission was submitted in June and was independently assessed by GIAA, who confirmed our self-assessment as accurate. Of the 47 outcomes, 7 were below expectations. These were all included in our DSPT Improvement Plan that we have been working on throughout the 2026/27. As at May 2026, we have completed 2 actions that have been agreed with GIAA, our 2025 auditors. We expect to complete 2 more before the end of June but will need to complete the final 3 after the summer, once Phoenix goes live and we have recruited additional IT resource.

21. We are currently finalising our 2026 DSPT, which is due for completion by the end of June. 12 standards will be independently evaluated as part of the submission, of which 9 are mandatory and 3 optional (where all 3 are ones where we had been below expectations in 2025). We procured a new auditor for the DSPT this year – MIAA[1], an NHS-based audit and assurance provider - from the NCSC's approved provider list. We went through an interim audit in April, with the final audit progressing in May. We are working with our auditor to bring as many of our outcomes as we can up to expectations by the end of June.

5. Information Governance activity in 2025/26

Data Subject Requests

[1] Miaa

22. In accordance with the UK GDPR, individuals have the right to exercise a number of data subject rights in relation to their personal data. These include the right of access, rectification, erasure, restriction of processing, data portability and objection to processing. The statutory timeframe for completion of these requests is one calendar month however, in specific circumstances this may be extended by a further two months, for example if the request is complex.

Subject Access Requests: 13

23. During 2025/26, the HFEA received 13 Subject Access Requests (SARs), all subject to the one-month legal response deadline. Of these, 11 were granted and three were denied.

24. Denials were issued on grounds where the information requested was not held on the HFEA Register and where thorough searches based on the details provided by the requester found no records within our database systems relating to the data subjects.

25. SARs can provide an alternative route for individuals to access some Register information. However, as SARs can only provide information strictly about the requesting individual, in several cases requesters were signposted to the OTR process if they were seeking to obtain Register data specifically. The majority of SARs received requested information about patients or donors regarding their treatment cycles, outcomes and donations.

26. SARs are becoming increasingly more frequent and complex, with an average of one to two requests received per month from August 2025 onwards, rising to a total of 5 requests in February 2026. In certain cases, the large volume of data held across multiple systems required considerable time and resources to identify, collate, manage and review the relevant data. A number of SARs received throughout the financial year involved complexities that required cross-team communication and input from Legal to support consistent decision-making and avoid both over- and under-scrutiny of requests.

27. Only three SARs did not meet the one-month deadline, due to the legal and operational complexity involved. In these cases we applied statutory extensions, in line with Article 12(3) of the UK GDPR, that can push back the deadline by a further two months. All remaining SARs were responded to within the legal timeframe.

Data Erasure Requests: 2

28. The HFEA received two data erasure requests at the start of the 202/26 financial year, which is unusual for the organisation. In response, a new standard operating procedure (SOP) is in drafting stages to support the handling of such requests. Both requests have been closed.

Data Rectification Request: 0

29. The HFEA's Information Governance did not receive any formal data rectification requests during the 2025/26 financial year.

Freedom of Information Requests (FOI): 64

30. In accordance with the Freedom of Information Act (FOIA) 2000, the HFEA, as a public body, is required to respond to requests from the public within 20 working days to promote transparency and support democratic principles. Furthermore, the ICO, in its responsibility to monitor compliance and set performance standards, has set an expectation that public authorities respond to at least 95% of FOI requests within the statutory time frame.

31. Our FOI KPI was met across the year. The complexity of FOIs this year has increased with requests mainly relating to clinic information, donation, human resources, IT, and finance.

32. During the 25/26 financial year, the HFEA answered 64 FOI requests. The HFEA missed deadlines for 3 FOI requests due to either the complexity of information requested or staff absence.

Month	Number of FOIs due	Number of FOIs that met target	Number of FOIs responded to
Apr-25	4	4	7
May-25	8	8	7
Jun-25	6	6	6
Jul-25	6	5	6
Aug-25	5	5	3
Sep-25	5	5	5
Oct-25	7	7	8
Nov-25	4	4	4
Dec-25	4	4	4
Jan-26	1	1	1
Feb-26	4	3	6
Mar-26	10	9	7
Total	**64**	**61**	**64**

Table 1: This table provides a monthly breakdown for the 2025/2026 financial year of the number of FOI requests due, the number responded to within the target timeframe, and the total number responded to in each month. Figures in this table may not align with FOI request numbers reported elsewhere, as this table only includes FOI requests responded to within the 2025/2026 financial year.

33. There were two Internal Reviews within the financial year.

    a. One Internal Review challenged the application of Section 12(1) 'Requests where the cost of compliance exceeds the appropriate limit' of

the FOIA 2000, following panel deliberation the engagement of this exemption was found to be appropriate.

b. One Internal Review challenged the application of several FOIA 2000 exemptions including: Section 44 ‘prohibition on disclosure’ and Section 40(2) ‘personal data’, Section 21 ‘information accessible by other means’, and Section 22 FOIA ‘information intended for future publication’. The panel agreed that the information requested was not for personal information, and therefore some of the exemptions (Section and Section 40(2)) were not appropriate. However, Section 36(2)(c) ‘prejudice to the effective conduct of public affairs’ was engaged then as the HFEA’s Qualified Person opinion stated that releasing the data would be likely to prejudice the effective conduct of public affairs. The panel upheld the original Section 21 exemption, because the requested data was already published through the archived webpages that were included in the original response. The application of Section 22 was also upheld as premature release would bypass necessary quality assurance and risk inaccuracy.

34. Following Internal Reviews, only one case was escalated to the ICO as a complaint, as of June 2026 the HFEA have not received any further communications from the ICO regarding this other than acknowledgement of receipt.

Environmental Information Regulations (EIR)

35. In accordance with the Environmental Information Regulations 2004, the HFEA, as a public body, is required to respond to requests for environmental information as soon as possible and no later than 20 working days after receipt of the request. Where a request is particularly complex and voluminous, the response period may be extended to 40 working days, provided the applicant is informed within the initial 20 working day period. Furthermore, the ICO, in its responsibility to monitor compliance and set performance standards, has set an expectation that public authorities maintain appropriate procedures to ensure timely, consistent and compliant handling of requests made under the EIR.

36. During the 25/26 financial year, the HFEA answered 1 EIR request within the statutory 20 working day deadline.

Data Breaches and Security Incidents

37. In the 2025/26 reporting year, the HFEA recorded 4 total data breaches and 3 near miss incidents. All reported data breaches were internal while 2 near miss incidents were external and were reported to the HFEA by clinics. Of all reported incidents only one confidentiality and data integrity breach was reported to the ICO within the statutory 72hr reporting period. This breach occurred as part of the donor’s address was visible to a recipient parent due to corruption in the attached PDF file. The case was closed with general recommendations from the ICO on improving redaction processes.

38. All breaches underwent a full data breach investigation and root cause analysis, with identified actions tracked to completion by the relevant manager. The common theme was unauthorised internal disclosure of personal data, often attributed to human error such as misdirected emails, incomplete redaction, or incorrect donor code assignment. Underlying causes included training gaps, high workloads, and insufficient procedural safeguards. Recommendations included SOP updates, targeted training, and increased staff awareness, particularly during high-pressure periods.

39. The number of reported breaches is not seen as a decline in standards, but rather as a positive reflection of greater staff awareness and improved incident reporting.

Data Protection Impact Assessments (DPIAs)

40. A Data Protection Impact Assessment (DPIA) is an important tool to ensure the HFEA manages personal information responsibly. A DPIA is relevant to initiatives involving the handling of personal information and should begin early in the life of a project, before any changes to processing have been made, and run alongside the planning and development process. It enables privacy considerations to be made early on in a project when any identified problems can be more easily resolved.

41. During 2025/26, only 2 projects have been deemed necessary for escalation to full DPIAs. 11 additional projects were submitted throughout the reporting year, however pre-DPIA screening confirmed no high-risk indicators were identified and therefore did not require a full DPIA.

6. Conclusion

42. We have a small and dedicated team of specialist staff that lead the HFEA's management of information and cyber security risk in a highly effective manner, but the context in which we manage our data is changing, as are the risks we face and the expectations placed upon us. We hold some highly sensitive data and the focus of our resource and efforts will continue to be the secure and compliant storage of these records.

43. In terms of the security of our data, the HFEA has appropriate cyber security in place, but we will need to continue working through our improvement programme over the coming year to ensure we are able to protect ourselves against changing threats and to recover from incidents in an efficient and effective way, with some additional internal resource and ideally some external support from DHSC and the CSOC.

44. I have considered the HFEAs compliance with the mandatory requirements set out in the 10 National Data Guardian (NDG) standards for data security[2]. These standards were designed to protect sensitive data and also protect critical services which may be affected by a disruption to critical IT systems (such as in the event of a cyber attack)

[2] [2] Data Security and Protection Toolkit assessment guides - NHS England Digital

and were the basis of the DSPT approach prior to alignment with the NCSC's Cyber Assessment Framework. This is contained at Annex B to this document. As can be seen, there are areas where we perform well, but there are also areas where we need to go further, which we will focus on as we continue to take forward our improvement plan after this year's DSPT assessment.

45. In conclusion I believe the HFEA has progressed well in its approach to data, information and records management over the past year and is in a stronger position in terms of its information governance and security as a consequence. As SIRO I believe the HFEA takes issues relating to information risk seriously and has appropriate processes in place to assess and minimise these risks. We will continue to maintain and improve processes over the coming year and ensure we consider how we can maximise the use of our information as a business asset.

Annex A

Information Governance and Cyber Security Steering Group - Terms of Reference

Aim

The Information Governance (IG) and Cyber Security Steering Group ('the steering group') is responsible for maintaining the confidentiality, integrity, and availability of data at the HFEA, and ensuring compliance with relevant laws and regulations.

Governance

The steering group will:

- have the powers to agree actions and policy changes relating to IG and cyber security
- work within the delegated budget limits of present Directors when setting direction and approving spend
- seek approval of the Corporate Management Group (CMG), the Senior Management Team (SMT) and/or the Audit & Governance Committee (AGC) where appropriate.

Functions

- Oversee the development, implementation and maintenance of IG and Cyber Frameworks, ensuring it remains current and fit for purpose.
- Ensure IG and IT security policies and procedures follow best practice, are effective and up-to-date; review staff compliance and awareness of these policies.
- Ensure compliance with the Data Security and Protection Toolkit (DSPT) and Cyber Assessment Framework (CAF) requirements, NHS guidance, and other applicable IG/cyber security standards; monitor progress against internal improvement plans.
- Assess data handling and security controls through member reports.
- Monitor IG and cyber threats, vulnerabilities, and risk posture; approve IG and cyber updates to the Strategic and Operational Risk Registers.
- Provide visibility of, and assurance that, Data Protection Impact Assessments (DPIAs) and security assessments are completed for any changes to the processing of personal data.
- Serve as the escalation point for IG and cyber security issues and risks.

- Oversee reporting, response, investigation, and analysis of cyber security/data incidents and near misses to inform training and support.
- Monitor and report on the number of data access and subject rights requests, identifying any response challenges.
- Discuss relevant legal and regulatory changes impacting IG and cyber security.
- Implement an IG, data protection and cyber security training programme for HFEA staff, aligned with the organisation's needs and best practice from the Information Commissioner Office (ICO).
- Promote a culture of IG and cyber security awareness and good practice across the organisation.
- Ensure cyber security is embedded in projects, systems, and procurement, aligned with Secure by Design principles and NHS/DHSC guidance

Roles and Responsibilities

Chair	Administrator	Lead Officer	Secretary
Director of Finance, Planning and Technology	Programme Support Officer	Senior Information Governance and Records Manager (IG) Head of IT (Cyber)	Head of Planning and Governance

The Steering Group shall follow the roles and responsibilities outlined in the HFEA Committee and Governance Groups Roles and Responsibilities document (CM 2025/009454).

Membership

Job title	Name	Role(s) on IG Steering Group
Director of Finance, Planning and Technology	Tom Skrinar	Chair Senior Information Risk Owner (SIRO)
Head of Planning and Governance	Sophie Tuhey	Secretary
Programme Support Officer	Arielle Nganya	Administrator
Head of IT	Martin Cranefield	Lead Officer (Cyber)
Senior Information Governance and Records Manager	Alice Collinge	Lead Officer (IG)
Data Protection Officer (DPO)	Jon Belcher [External]	DPO
Director of Compliance and Information	Rachel Cutting	Member

Head of Information	Neil McComb	Caldicott Guardian
IT Service and Systems Manager	Karl Saunders	Member
Risk and Business Planning Manager	Shabbir Qureshi	Member
Information Governance and Records Management Officer	Sinead O'Boyle	Member

The Head of Research and Intelligence and Information Asset Owners may be invited to attend by invitation.

Agenda

IG Steering Group		
	Item	**Lead**
1.	**Actions from previous meeting**	Chair
2.	**IG / records management /Cyber updates:** • SharePoint migration • Changes to data storage/processing • System changes	Senior IG and Records Manager / Head of IT
3.	**Horizon scanning:** • Legislative changes affecting IG and emerging guidance/best practice • Legislation changes affecting cyber security and emerging guidance/best practice	DPO / Senior IG and Records Manager
4.	**Reports and metrics** • Data breaches/near misses: trends, mitigations, lessons learned • Data subject rights requests, information access requests; FOI; volume, challenges • Data Protection Impact Assessments undertaken • Cyber security incidents / near-misses: trends, mitigations, lessons learned	Senior IG and Records Manager / Head of IT
5.	**Risk Management** • Escalated open risks related to IG • Escalated open risks related to cyber security	SIRO / IAOs (where applicable)
6.	**Policies and staff training** • Policy/SOP review	Senior IG and Records Manager /

	• Training Needs Analysis • Compliance rates	Head of IT
7.	**Data Security and Protection Toolkit (DSPT):** • Review progress against DSPT / Information Security Improvement Plan • Review audit recommendations • Review compliance with Secure by Design policy and principles	Head of Information / Head of IT
8.	**AOB**	All

Administration

Frequency	• Quarterly, with additional meetings as required (e.g. following major breaches or incidents). • 2 hours in duration • Ideally meetings will happen 4-6 weeks before AGC
Format	Meetings will usually be held remotely
Attendance	• Each member to appoint a substitute, where appropriate, for any meetings they are unable to attend. • Other staff may be invited to attend on occasion.
Papers and presentations	• Papers to be as concise as possible using HFEA branding/ templates. • Papers to be submitted to the Administrator and distributed to the group at least 5 working days prior to the meeting. • Papers to clearly articulate recommendations and any decisions to be taken.
Minutes and actions	• Formal minutes will not be taken (notes and actions only) • Outstanding actions will be reviewed at each meeting. • Notes and actions distributed within 5 working days after each meeting. • Summary presented to CMG by Chair each quarter.
Reporting	The steering group shall report to: **The Audit and Governance Committee (AGC)** • on a quarterly basis • to provide a summary of IG and cyber security updates • to provide an annual summary of performance compliance **Senior Management Team (SMT)** • as required • to escalate significant risks, incidents, or compliance failures **Corporate Management Group (CMG)** • as required

- to inform top 3 operational risks, resources and prioritisation
- for policy clearances

The steering group will also provide updates and reports to HFEA staff as appropriate (e.g. Hub posts).

Version/revision control

Version	Changes	Updated by	Approved by	Release date	Review date
1.0	Terms of Reference drafted	Sophie Tuhey	Name, role	04/09/2025	01/09/2026

Annex B – Assessment of the HFEA's compliance with the mandatory requirements set out in the 10 National Data Guardian (NDG) standards for data security

	Mandatory Requirement	Compliance	Further actions required
1	**Personal confidential data** is only shared for lawful and appropriate purposes. Staff understand how to strike the balance between sharing and protecting information, and expertise is on hand to help them make sensible judgments. Staff are trained on relevant legislation and periodically reminded of the consequences to patients and service users, their employer and to themselves of mishandling personal confidential data.	We have internal protocols (including DPIAs, SOPs and staff acting in advisory capacity) to reach sensible judgments considering relevant information. All staff undergo mandatory data protection awareness e-learning, which is refreshed on an annual basis.	Implementation of privacy compliance software and additional resource to help us to design more tailored training modules which will be delivered on a regular basis/available on demand
2	**Staff responsibilities.** All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches. All staff understand what constitutes deliberate, negligent or complacent behaviour. Insecure behaviours are reported without fear of recrimination and procedures which prompt insecure workarounds are reported, with action taken.	Staff responsibilities are clearly included in employment contracts and policies, including the HFEA Staff Code of Conduct, Acceptable Use Policy, Information Security Policy and Incident Reporting Policy.	Review of this suite of policies, including any gaps identified through external support or DSPT review to reinforce a security culture in the organisation.
3	**Training.** Staff have appropriate understanding of information governance and cyber security, with an effective range of approaches taken to training and awareness	The HFEA has a focused Training Needs Analysis that is reviewed by the IG Steering Group. All staff undergo mandatory data protection awareness e-learning, which is refreshed on an annual basis.	Implementation of privacy compliance software and additional resource to help us to design more tailored training modules which will be delivered on a regular basis/available on demand
4	**Managing Data Access.** Personal confidential data is only accessible	We control this by applying permissions only when	We will consider our position here in

	Mandatory Requirement	Compliance	Further actions required
	to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.	required and always used named accounts	response to a consultancy review of our processes that began in January 2026
5	**Process Reviews.** Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security	When breaches or near misses are identified, relevant SOPs are reviewed to prevent reoccurrences	SOP annual reviews are not currently formally tracked or monitored. We will explore the possibility of automatic notification during the SharePoint records management design phase
6	**Responding to Incidents.** Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection. All staff are trained in how to report an incident. Basic safeguards are in place to prevent users from unsafe internet use. Anti-virus, anti-spam filters and basic firewall protections are deployed to protect users from basic internet-borne threats.	The HFEA developed new Business Continuity and Critical Incident Response plans in 2024/25, with an understanding that senior management would be informed within 12 hours.	We reviewed and tested our plans in summer 2025 but have further work to do looking at managing incident responses (in partnership with the NHS CSOC) and refining our recovery planning. This should be supported with external consultancy.
7	**Continuity Planning.** A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.	The HFEA developed new Business Continuity and Critical Incident Response plans in 2024/25.	We reviewed and tested our plans in summer 2025, but have further work to do looking at managing incident responses (in partnership with the NHS CSOC) and refining our recovery planning. This should be supported with external consultancy.
8	**Unsupported systems.** No unsupported operating systems,	The HFEA has some key legacy systems that we are currently updating, in particular	This work should complete by the end of summer 2026.

	Mandatory Requirement	Compliance	Further actions required
	software or internet browsers are used within the IT estate.	epicentre, our inspection and licensing software.	
9	**IT Protection.** A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as cyber essentials. This is reviewed at least annually.	We deploy protection in various forms e.g. device endpoint management (monitoring and anti-virus protection); email security (malware and phishing filtering); Azure security (cloud monitoring systems)	We will consider our position here in response to a consultancy review of our processes that began in January 2026, as well as ongoing discussions with the NHS CSOC
10	**Accountable Suppliers.** IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.	Hold all third-party suppliers and data processors accountable through appropriate contracts and due diligence	Use of data protection software to aid data flow mapping and to monitor progress on this Further work based on alignment with Secure by Design and Privacy by Design approaches, focussed on project and procurement approach as well as contracting.

Human Fertilisation & Embryology Authority

PEOPLE STRATEGY Update June 2026

Progress to date

Yvonne Akinmodun
Head of HR

www.hfea.gov.uk

A snapshot of our workforce

88	15.4%	2.01%	60%
Total Headcount	**Turnover Rate**	**Avg Sickness**	**Home Workers**
As at 31 March 2026	13 leavers (15 inc. planned)	April 2022 – March 2023	53 home / 35 office-based

17	13	2
New Starters	Leavers Processed	Retirements / Ill-health Ret.

As at the 31 March 2026, the HFEA had 88 active staff in post and a total headcount of 92 staff. Turnover of 15.4% is slightly above our 15% KPI target, however we anticipate that turnover will plateau on the next few months . Sickness absence at 2.01% is below the public sector average of 2.5%, reflecting positively on staff wellbeing. 60% of the workforce are home-based, with the remainder office-based.

Human Fertilisation & Embryology Authority

Our People Strategy at a glance

Our People Strategy launched in April 2025, setting out our ambition to build a high-performing, inclusive and resilient organisation.

- **Resourcing & Recruitment**
- **Employee Development**
- **Leadership Capability**
- **Diversity, Inclusion & Wellbeing**
- **Organisational Resilience**
- **HR Service Delivery**

Human Fertilisation & Embryology Authority

Progress highlights since launch

Resourcing	Search for a new HR is system scheduled to begin in summer 2026. Refresh of our values and behaviour in preparation for future recruitment processes in development.
Learning & Development	Skills audit completed along with the annual training plan. Work shadowing program launched to support employee career development journey.
Leadership	Leadership development plan is being developed. Career conversations workshop for leaders scheduled for the summer. ILM program launched in January 2026
EDI & Wellbeing	Wellbeing and EDI champions in place. Work from the Office Day indicative launched to support wellbeing, with good take-up. Bi-annual wellbeing pulse survey planned for launch in June.
Organizational Resilience/ Workforce Planning	Establishment control tools in place. Skills audit completed.

Road map status

Short · Medium · Long Term

SHORT TERM
2025–2026 (completed)

- Skills audit & gap analysis
- Work shadowing programme launched
- Wellbeing champions in place
- Refreshed values & behaviors
- Bi-annual wellbeing pulse survey starting June 2026
- Leadership development program developed, awaiting roll out

MEDIUM TERM
2026–2027 (Planned or in progress)

- HR system review
- Leadership development program roll out
- Wellbeing Plan design and launch
- Aspiring Manager Program
- Review PDP policies & processes
- Values & behaviour recruitment process designed and rolled out

LONG TERM
2027–2028 (Not started)

- ATS system search & procurement
- Pay & reward strategy review
- EDI action plan launch
- Organisation -wide 360 feedback program
- 2026/27 activities reviewed to inform next 3 -year strategy

Human Fertilisation & Embryology Authority

Key Focus Areas

Priorities for 2026–2027

01 Aspiring Manager Programme

Planning underway — launch the programme to develop new and emerging people leaders.

02 Leadership Development Plan

Finalise and begin delivery of the leadership development plan across the organisation.

03 Wellbeing and EDI

Implement the bi-annual wellbeing pulse survey to provide ongoing data to guide wellbeing actions. Development of our wellbeing plan.

04 HR System Procurement

Begin the search for a HR system with stronger data capture and reporting capability, in particular in the area of L&D. Search to commence in the summer of 2026

05 ATS Procurement

Begin the search for a new applicant tracking system to modernise recruitment from early 2027.

Human Fertilisation & Embryology Authority

HR Service Delivery

Key achievements for 2025–2026

01 Resourcing & Recruitment

In the last 12 months, we ran 18 recruitment campaigns with an average advert to hire time of 30 days (Sector average is 56 day)

02 Employee Development

In the last 12 months, we have led over 20 L&D initiatives spanning development, wellbeing & HR operations

.

03 Leadership Capability

We created a leadership development and also introduced an ILM pilot

04 Diversity, Inclusion & Wellbeing

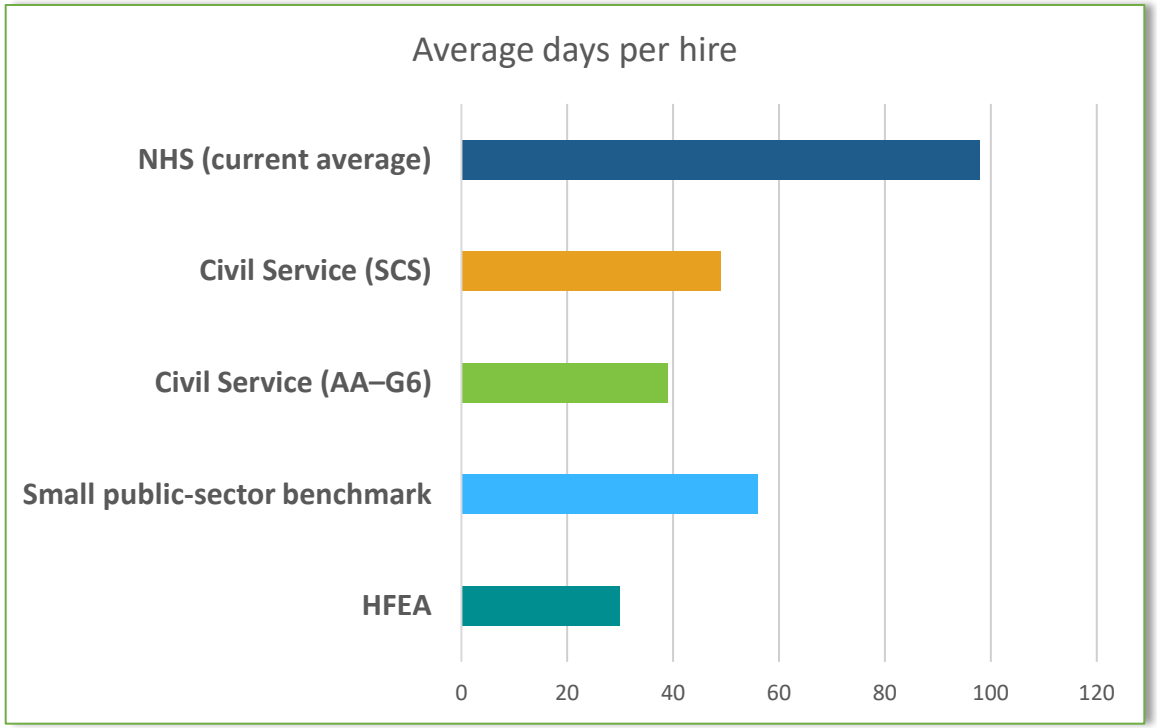
Staff retention & wellbeing audit measured well against civil service standards. Our staff survey completed in 2025/26 with an engagement score of 83% and an award for the second year running.

05 Organizational Resilience

Completion of skills audit and the creation of a corporate training plan. introduction of HR dashboard to increase visibility of key HR activities. Annual review and update of key HR policies

Human Fertilisation & Embryology Authority

Time to hire within the HFEA compared with public sector



Sector / benchmark	Typical time to hire (Days)	Average
HFEA	**24 -41 days**	**30**
Small public-sector benchmark	**42–70 days**	56
Civil Service (AA–G6)	**17–61 days (median)**	39
Civil Service (SCS)	**28.5–70 days (median)**	49
NHS (current average)	**~98 days (≈14 weeks)**	98

HFEA's average time to hire (30 days) is substantially faster than all public-sector comparators, performing well below the small public-sector benchmark (56 days) and ahead of both Civil Service and NHS averages. Overall, HFEA's recruitment timeline reflects strong efficiency by public-sector standards.

Human Fertilisation & Embryology Authority

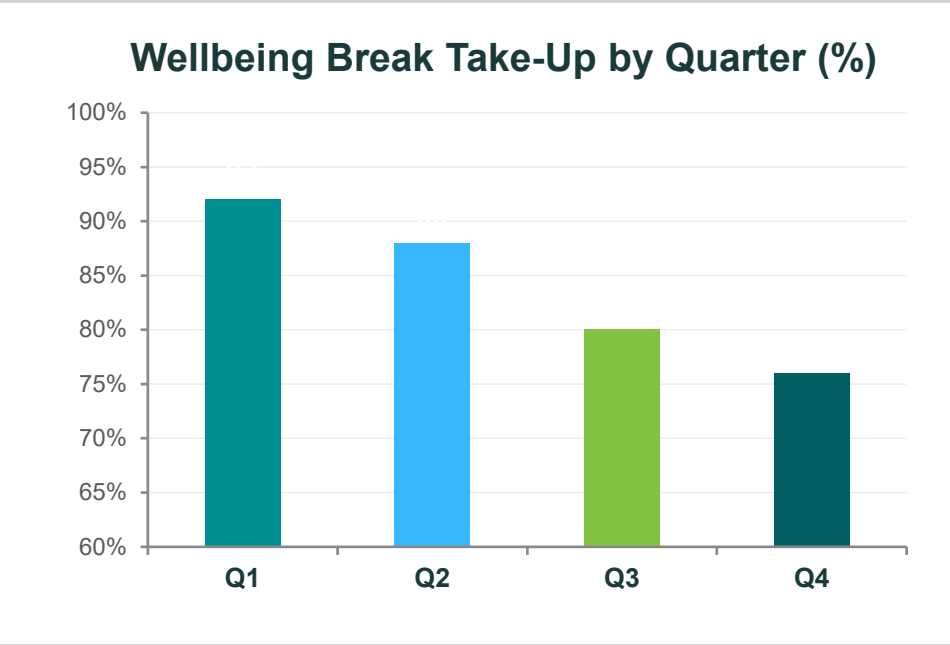
HR Operations

12 Month Data
01 April 2025 – 31 March 2026

Policy Updates This Year
10
↑ 3 vs prior year

New HR Initiatives Launched
6
On track: 5 | In progress: 1

Wellbeing Break Take-Up Rate
73%
Target: 80%



In quarter one, we recorded the highest take up of wellbeing breaks; 92%. However since then, the data shows a steady decline in the take up of wellbeing with a record of 76% in quarter four. We believe this decline is likely to be as a result of under recording. Managers will be encouraged to remind staff of the necessity of recording time take off for wellbeing breaks so that the data can effectively be captured and reported.

Policy updates include new policies issued and substantive revisions to existing policies.

Learning & Development

12 Month Data
01 April 2025 – 31 March 2026

Total Courses (Excluding Mandatory) Delivered

15

↑4 vs prior year

Total Learners (Unique)

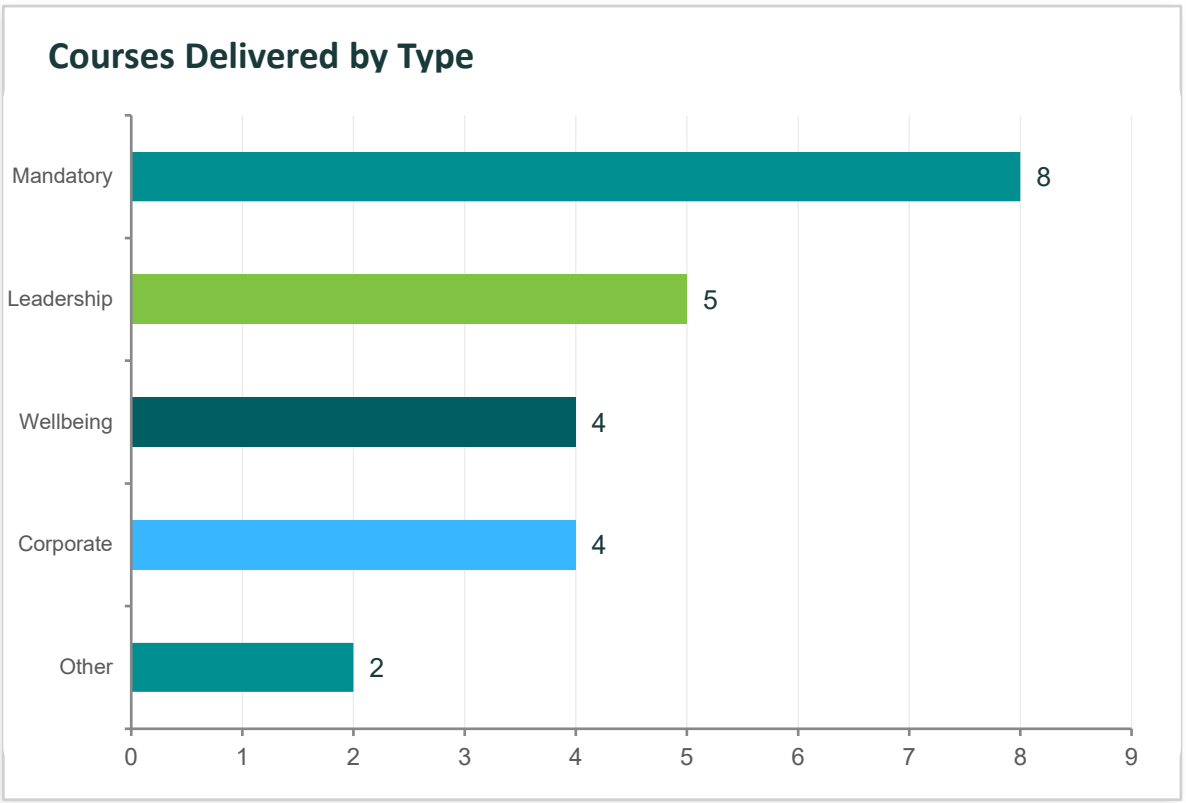
43

Excluding Mandatory training

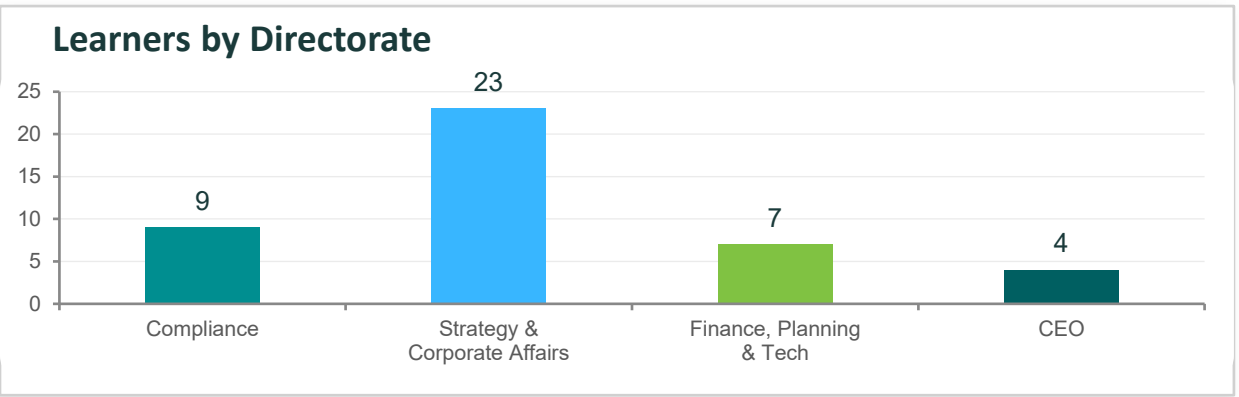
Current Completion rate for mandatory training as at May 2026. Deadline – Aug 2026

37%

Courses Delivered by Type



Learners by Directorate



Learner counts reflect unique individuals. Hours data covers internal and externally facilitated programmes.

Human Fertilisation & Embryology Authority

HR Service Delivery - Our HR Dashboard

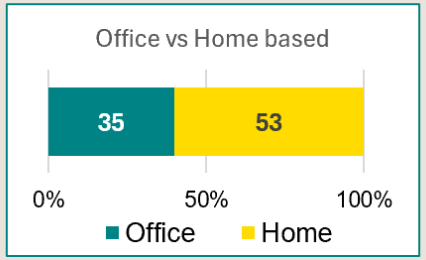
HR Dashboard - All Departments

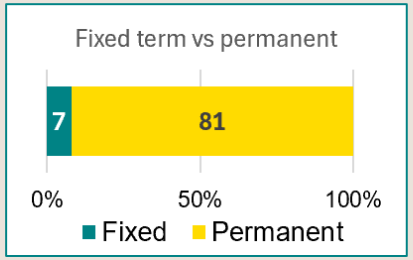
Month selected: Mar 2026

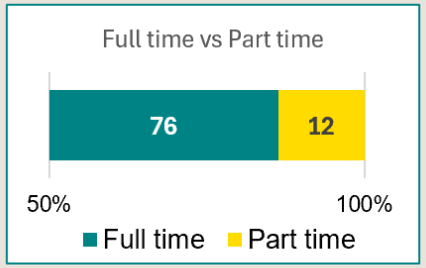
Human Fertilisation & Embryology Authority

Employment Status

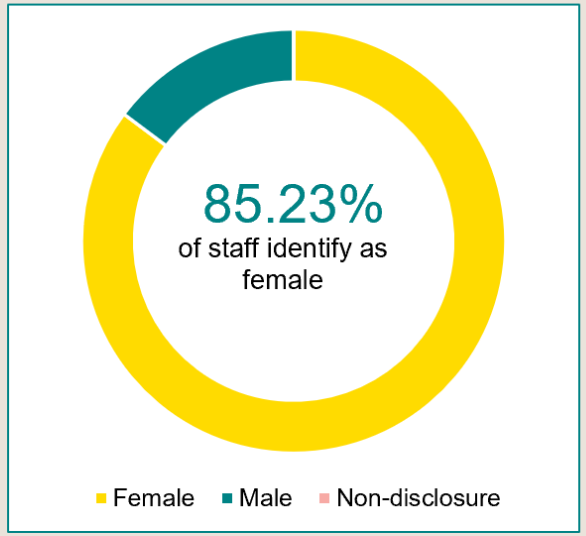
Total Staff	Turnover Rate	Vacant Posts
88	0.00%	2
+1% vs previous month	New starters: 3 Leavers:	



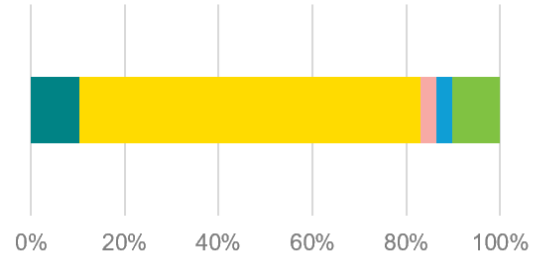




Equality and Diversity



72.73% of staff identify as white



Disability Status
7.95%
of staff self-describ as having a disability

Productivity

Sickness Rate	Training Days
0.00%	#VALUE!
-6.11% vs previous month	vs previous month

Audit & Governance Committee Forward Plan

Details about this paper

Area(s) of strategy this paper relates to:	Regulating a changing environment / Supporting scientific and medical innovation
Meeting:	Audit & Governance Committee
Agenda item:	15
Meeting date:	16 June 2026
Author:	Morounke Akingbola, Head of Finance
Annexes	

Output from this paper

For information or decision?	For decision
Recommendation:	The Committee is asked to review and make any further suggestions and comments and agree the Forward Plan.
Resource implications:	None
Implementation date:	n/a
Communication(s):	n/a
Organisational risk:	Low Not to have a plan risks incomplete assurance, inadequate coverage or unavailability of key officers or information

Audit & Governance Committee Forward Plan

AGC items Date:	**16 June 2026** **In-person**	**13 Oct 2026** **Virtual**	**2 Dec 2026** **In-person**	**Feb/March 2027**	**June 2027**
Following Authority Date:	**1 July 2026**	**18 Nov 2026**	**Jan 2027**	**March 2027**	**July 2027**
Internal Audit	Results, annual opinion, internal audit charter Potentially: consider auditees feedback	Update - mid year review of audit plan	Update	Approve draft plan	
Internal Audit Recommendations Follow-up	Yes	Yes	Yes	Yes	
External audit (NAO) strategy & work	Audit Completion Report		Early reflections report on the financial statements audit		
Session for Members and auditors	Yes	Yes	Yes	Yes	
Annual Report & Accounts (including Annual Governance Statement)	Yes, for approval				
Strategic Risk Register	Yes	Yes	Yes	Yes	

AGC items Date:	**16 June 2026 In-person**	**13 Oct 2026 Virtual**	**2 Dec 2026 In-person**	**Feb/March 2027**	**June 2027**
Risk Management Strategy1			Yes	Yes	
Horizon scanning committee discussion	Yes	Yes	Yes	Yes	
Deep dives		CaFC / PRISM		Patient complaints	
Digital Programmes Update	Yes	Yes	Yes	Yes	
Resilience & Business Continuity Management	Update as necessary	Update as necessary	Update as necessary	Update as necessary	
Information Assurance & Security	Yes, plus SIRO Report				
HR, People Planning & Processes	Bi-annual HR report		Bi-annual HR report		
Contracts & Procurement including SLA management	Update as necessary	Update as necessary	Update as necessary	Update as necessary	
Whistle Blowing, fraud (report of any incidents)	Update as necessary	Update as necessary	Update as necessary	Update as necessary	
Estates	Yes				
Review of AGC effectiveness and		Yes	Yes		

1 Policy will have been reviewed by the Executive, including updated appetite statement for Authority approval.

AGC items Date:	**16 June 2026 In-person**	**13 Oct 2026 Virtual**	**2 Dec 2026 In-person**	**Feb/March 2027**	**June 2027**
terms of reference					
Functional standards	Yes	Update as necessary	Update as necessary	Update as necessary	
AGC Forward Plan	Yes	Yes	Yes	Yes	
Accounting policies				Yes (annually)	
Public Interest Disclosure (Whistleblowing) policy				2028	
Counter fraud and anti-theft policy				2028	
Counter-fraud Strategy (CFS), Fraud Risk Assessments (FRA) and progress of Action Plan		Yes			
Reserves policy		Yes			
Dear Accounting Officer letters	Update as necessary	Update as necessary	Update as necessary	Update as necessary	
Meeting specific items	Private meeting SMT and AGC members		Training session in the afternoon		Private meeting SMT and AGC members

Training topics

This list below are suggested topics which could be considered for AGC members

- Risk Management
- Counter fraud
- Cyber Security - proposed for December 2026

Suggested deep dive topics

Suggested topic	Date added	Potential meeting to be discussed
CaFC/PRISM	27 June 2023	October 2026
Patient's complaints about licensed clinics	14 Oct 2025	February 2027
Deep dive/lessons learned from the closure of the next critical incident	24 Feb 2026	

Version/revision control

Version	Changes	Updated by	Approved by	Release date	Review date
1.0					

Gifts and Hospitality Register

Details about this paper

Area(s) of strategy this paper relates to:	Regulating a changing environment
Meeting	AGC
Agenda item	16
Meeting date	16 Juney 2026
Author	Morounke Akingbola, Head of Finance

Output from this paper

For information or decision?	For information
Recommendation	AGC is invited to note thee declarations within the register
Resource implications	N/a
Implementation date	2026/27 business year
Communication(s)	Na
Organisational risk	Low

Introduction

The Declaration of Interests and Gifts and Hospitality is a standing item on the agenda. The register will only be presented when there are new items added.

Update

The register at Annex A contains two new items since the February 2026 meeting.

Action

The committee are requested to note the register contents.

Register of Gifts / Hospitality Received and Provided/Declined

Version: HFEAG0001
Jun-26

DIVISION / DEPARTMENT: HFEA
FINANCIAL YEAR: 2026/27

	Details of the Gift or Hospitality						Provider Details			Recipient Details	
Type	**Brief Description of Item**	**Reason for Gift or Hospitality**	**Date(s) of provision**	**Value of Item(s)**	**Location where Provided**	**Action on Gifts Received**	**Name of Person or Body**	**Contact Name**	**Relationship to Department**	**Name of Person(s) or Body**	**Contact Name**
Either 'Provision' or 'Receipt'	*Give a brief description of the gift or hospitality recorded*	*Summarize the reason or occasion for the gift or hospitality*	*Give the date(s) on which it was provided or offered*	*Give the known or estimated value - if unknown then state 'unknown' and explain further under the 'Reason for Gift' column.*	*Give the name of the venue or location at which the gift or hospitality was provided*	*For Gifts Received only, specify what happened to the item(s) after it was received*	*Give the name of the individual or organization providing or offering the gift / hospitality*	*Give a contact name if an individual is not specified as the provider - otherwise leave blank*	*Specify the relationship of the provider to the Department (e.g. 'supplier', 'sponsor', etc.) - if the Department is the provider then leave blank*	*Give the name of the individual(s) or organisation receiving the gift / hospitality - if there are multiple recipients, specify each on a separate line*	*Give a contact name if an individual is not specified as the recipient - otherwise leave blank*
Receipt	Hospitality at private home	Invitation to review AI models for IVF treatment developed from data collected over 30 years	18/04/2026	Nk	Cotswolds	Accepted	ARGC Ctrs 0088/0157/0206	Muhamad Taranissi	Licenced centre	Rachel Cutting	
Receipt	M&S Voucher	Speaking at BICA conference	15/05/2026	£ 30.00	Mary Ward House	Accepted	BICA Annual Conference			Clare Ettinghausen	