Witness Statement Number: WITN0226001

Witness Name: Manjeet Shehmar

Dated: 5 December 2025

NOTTINGHAM INQUIRY

First Witness Statement of Dr Manjeet Shehmar

I, Dr Manjeet Shehmar, will say as follows -

INTRODUCTION

1 I am currently Medical Director and Responsible Officer to the GMC at Nottingham University Hospitals NHS Trust ('the Trust') and have been in this role since July 2024.

2 I am a Consultant in Obstetrics and Gynaecology, and I graduated from Imperial College School of Medicine in 1998.

3 Prior to joining the Trust, I worked at Birmingham Women's and Children's NHS Foundation Trust as Clinical Director for Gynaecology, Theatres and Fertility between 2014 and 2019. In 2019 I joined Walsall Healthcare NHS Trust as Deputy Medical Director, before being appointed as their Chief Medical Officer.

4 On 13 June 2023, Valdo Calocane killed three people and seriously injured three others ('the Incident'). These individuals were all admitted to the Queens Medical Centre Emergency Department and variously treated.

5 We are currently investigating concerns that members of staff of the Trust may have inappropriately accessed the medical records of Ian Coates, Grace O'Malley Kumar and Barnaby Webber. When we became aware of the potential unauthorised access to medical records we complied with our duty of candour and have been keeping the families updated and will continue to do so throughout our investigation. Following further correspondence with

representatives of survivors of the attacks that were also cared for at our hospitals we began investigating concerns that their records may also have been accessed inappropriately in March 2025.

6 The families of Ian, Grace and Barnaby, as well as the survivors of the attacks, have already had to endure much pain and heartache and we are truly sorry that this will add further to their suffering. We fully acknowledge the seriousness of the concerns raised and our responsibility to protect the privacy of service users. Through our investigation, we will find out what happened and will not hesitate to take action as necessary.

7 The Trust have been asked a number of questions in relation to unauthorised access to and disclosure of information generated following the Incident, as well as the handling of communication with both survivors and the bereaved families of the victims of the Incident. This statement reflects the position as at 15 July 2025, the point of submission of the statement in draft form to the Inquiry. Accordingly, all references to current circumstances, ongoing matters, and the present tense, should be understood as referring to the position as at 15 July 2025.

8 At the time of the incident, I was not in my current role as Medical Director of the Trust but was in my role at Walsall Healthcare NHS Trust. I was not involved in either the delivery of care to the victims of the Incident or handling of the information generated as a result. I am giving this statement in my current position as the Medical Director of the Trust and my role in the investigation of the identified potential unauthorised access to the medical records of the victims of the Incident. As is reflected in this statement below, I have been involved in this incident since the Trust became aware of potential unauthorised access to records by members of its staff, liaising initially with counterparts at Nottinghamshire Healthcare NHS Foundation Trust, the Trust Caldicott Guardian, and then being appointed as the Strategic Commander of the Incident Command Group that was established within the first days of the Trust becoming aware of these concerns to oversee the investigation and broader

handling of this matter by the Trust. I have therefore had oversight of this matter in this role and continue to work closely with the Caldicott Guardian and other key individuals of the Trust in the handling of this matter.

9 A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patients' health information and making sure it is used properly. The Trust's Caldicott Guardian at the time of the Incident (and currently) is Dr Jeremy Lewis.

10 This statement is the product of drafting after communications between me and Browne Jacobson LLP in writing, by telephone and video conference. I have relied on information and the documents provided by several senior individuals within the Trust, including Jeremy Lewis (Caldicott Guardian), Gilbert George (Director of Corporate Governance), Marc Wilson (Data Protection Officer), Myles Timson (Head of Employee Relations), Deborah Gladden Porter (Deputy Director of People – Operations and Governance), Andy Callow (Chief Digital and Transformation Officer, and Senior Information Risk Owner), Lisa Lawrence (Deputy Director of Digital Services) and Eleanor Jones (Training and Registration Authority Manager). In accordance with Trust internal governance processes this statement has been considered by the Trust Chair, Nick Carver OBE and Chief Executive, Anthony May OBE DL under delegated authority from the Trust Board prior to its submission.

11 I am the appropriate witness to address the Rule 9 Request because of my role in the investigation into unauthorised access to records, as the Strategic Commander of the Incident Command Group and the Trust's Medical Director. Where matters are outside my direct knowledge, I am well-placed to obtain and provide that information to the Inquiry via liaison with the relevant colleagues, as explained above.

12 This statement sets out my response on behalf of the Trust to the questions asked by the Inquiry in the Rule 9 request dated 3 June 2025. It has been drafted on my behalf by Browne Jacobson LLP with my oversight and input.

Browne Jacobson LLP are acting as, and respectfully request that the Inquiry appoint them as, the Trust's Recognised Legal Representative.

13 The contents of this statement are true to the best of my knowledge, information and belief.

14 Producing this statement has required a targeted review of documents collated by the Trust to date. I understand from communications between Browne Jacobson LLP and the solicitor to the Inquiry that a targeted approach to disclosure is sought by the Inquiry, exhibiting only key documents in relation to this matter. The Trust will notify the Inquiry if information comes to light that would have been included in the statement if I had been aware of it at the time of drafting.

APPROACH TO RESPONDING TO THE RULE 9 REQUEST

15 I have sought to answer all questions of the Inquiry as posed in the Rule 9 request dated 3 June 2025. I have not adopted a "question and answer" format in responding to those questions but have instead adopted a narrative approach. This approach better enables the Inquiry to fully understand the response of the Trust, including when and why any steps were taken, and is intended to assist the Inquiry in its overall understanding of the Trust's handling of this matter. I have set out the response to the Rule 9 request in the following manner:

a) A summary of the Trust's position as further detailed in the following sections of this statement.

b) An overview of the Trust.

c) The relevant applicable legal and national policy context in which the Trust operates.

d) The controls in place within the Trust to prevent the unauthorised or illegitimate access to medical records, including from a systems perspective and guidance/policy perspective.

e) The factual and chronological position regarding the Trust's awareness of potential unauthorised access to records of the victims of the Incident, and the Trust's handling of this matter, including communications with the surviving victims and bereaved families.

f) What the Trust has learned from this matter and steps intended to be taken going forwards.

SUMMARY POSITION OF THE TRUST

16 The Trust first came into possession of information relevant to the victims of the Incident on 13 June 2023 when they were admitted to the Trust Emergency Department. In respect of the deceased victims (who were either sadly deceased on arrival or shortly thereafter) the Trust holds relatively little information generated after 13 June 2023. The position is different in relation to the surviving victims, all of whom have received further treatment from the Trust following the Incident.

17 Despite being in possession of relevant information from 13 June 2023, the Trust did not become aware of any suggested unauthorised access until early October 2024 when an audit request was made by Nottinghamshire Healthcare NHS Foundation Trust. This request was made only in the context of Nottinghamshire Healthcare NHS Foundation Trust being the employer of certain individuals who also worked at the Trust's Queen's Medical Centre site and who would therefore also have access to records held on the Trust's systems. Nottinghamshire Healthcare NHS Foundation Trust received correspondence from a solicitor acting on behalf of the bereaved families requesting confirmation of who had accessed the records of the deceased victims. A request for the same information was subsequently made by the Medical Director of Nottinghamshire Healthcare NHS Foundation Trust directly

to the Caldicott Guardian of the Trust. During this period there were two distinct lines of enquiry which were ongoing with it only later being realised that this was the case. It was at this point that the Trust conducted audits of its relevant systems, and it became aware of potential unauthorised access to the medical records of the deceased victims by a number of staff employed by the Trust.

18 Having identified this concern, the Trust responded with the Caldicott Guardian undertaking an initial screening of audit reports of relevant Trust systems to seek to understand the potential extent of unauthorised access to records and making an early referral to the Information Commissioner's Office. I was made aware of the issue in my role as Medical Director, and an Incident Command Group was established to ensure the appropriate handling of the matter from the perspective of communicating with the families, reporting to relevant third-party bodies, further investigation, and that appropriate disciplinary processes were conducted where appropriate.

19 During the period that followed, the Trust informed the bereaved families of what was understood to be the unauthorised access to records of the deceased victims pursuant to its duty of candour obligations, and referrals were made to a range of bodies including NHS England, NHS Nottingham and Nottinghamshire Integrated Care Board, Nottinghamshire Police, and the General Medical Council.

20 Having informed the bereaved families of the concerns of the Trust, a candid approach was adopted whereby regular updates as to the ongoing investigative processes of the Trust were delivered initially on a weekly basis and subsequently, with agreement, fortnightly to the bereaved families' solicitor. Comments from the families were also sought in relation to terms of reference in respect of different elements of the investigative process described further below.

21 Whilst the Trust accepts that there is always room for improvement in the handling of any matter, it is confident in the position that has been adopted with

regard to the communication with the bereaved families in this current matter. The Trust has complied with its duty of candour, and adopted an open and transparent approach which ensures that the bereaved families are kept informed of progress in relation to the handling of this serious matter, as well as enabling an appropriate degree of involvement in the processes being undertaken to ensure that the bereaved families feel satisfied as to the approach adopted by the Trust and the ultimate outcome of the process. The Trust genuinely values the input it has received from the bereaved families and surviving victims into the processes it has adopted, and which have helped to ensure a robust and proportionate approach to this matter and expresses its gratitude for their involvement in what is recognised to be a very difficult circumstance.

22 A two-stage process was established for the identification and investigation of potential unauthorised access to records. Stage 1 of this process involved managers of staff under consideration, conducting fact-finding interviews and completing a proforma document which was then considered by an appointed multi-disciplinary Task and Finish Group, who determined whether the case was to proceed to Stage 2. Stage 2 involved an independent, third-party investigator (a former Human Resources Director) conducting a more detailed exercise and reporting to the Trust as to whether they considered there to be a case for potential disciplinary action. This would then inform as to any disciplinary process undertaken within the Trust. These processes remain ongoing at the point of submission of this statement, though some of the Stage 1 and Stage 2 processes for those staff that accessed the records of the deceased victims are complete (subject to five outstanding cases) and reports have been received from the independent investigator.

23 Whilst the process in relation to potential unauthorised access to records of the deceased victims was ongoing, concerns were subsequently raised by two of the three surviving victims on 21 March 2025, via appointed solicitors, as to whether there had also been unauthorised access to their records. Up to this

point the Trust had focussed on taking action to address the concerns raised in relation to the deceased victims and mitigating the risk of further unauthorised access and in this context had not at that stage considered the potential for unauthorised access to others potentially related to the Incident. Upon the concern being raised the Caldicott Guardian conducted an initial screening exercise and formed the opinion that the records of these victims of the Incident had also been accessed without legitimate purpose by a number of staff of the Trust. Similarly to the concerns raised by the bereaved families of the deceased victims, the Trust complied with its duty of candour obligations to the surviving victims, as well as reporting to the various third-party bodies previously informed in respect of the unauthorised access to records of the deceased victims. The same two-stage investigative process was commenced in relation to the access to records of the surviving victims, and Stage 1 remains ongoing.

24 It is noted that the Inquiry has specifically referred to both the issue of the management of video footage and evidence in the investigation and prosecution of high-profile cases. This issue is not considered to be relevant to the Trust which does not have prosecution powers. The Trust has considered whether there has been any illegitimate access to CCTV footage of the arrival of the victims of the Incident at the Trust Emergency Department. The Trust has found no evidence of this.

25 The Inquiry has also referred to inappropriate telephone messaging. The Trust's investigations to date have not revealed any evidence of this, nor evidence of any records having been extracted or disclosed from its systems. The concerns of the Trust relate only to the issue of unauthorised access to records and so this statement is focussed on only this issue.

26 The Trust considers that upon becoming aware of the potential unauthorised access to medical records by staff of the Trust it acted appropriately, in accordance with its statutory duties, the rights of the bereaved families and the surviving victims. The bereaved families and surviving victims were informed

of the concerns of the Trust and have been kept informed as investigations have progressed. Only one of the surviving victims is unrepresented and has agreed to be informed at the outcome of the process being undertaken by the Trust.

27 The Trust recognises that there is learning to be taken from this along with previous instances of staff members accessing patient records without a legitimate reason for doing so. The Trust has taken action during the course of its investigation of this matter and intends to take further steps to identify any additional action that can or should be taken going forwards.

28 The steps taken during the course of the investigative process include sending a number of communications to staff across the Trust specifically on the issue of unauthorised access to medical records, conducting checks against the records of the deceased and surviving victims of the Incident on a fortnightly basis to identify whether there has been any further unauthorised access to these records (of which there has been none identified), and making an amendment to systems access controls so that front desk receptionists at Queen's Medical Centre are restricted to only viewing patient location information (it being identified that up to this point they had standard ward receptionist access).

29 The Trust has explored the options available to it to improve its core patient systems, with the potential to "lock down" records or impose additional access controls (such as a "challenge" to indicate the justification for access) within those systems. The core patient administration system functions of the Trust are to be transferred in October 2025 from its current system, Careflow, to the system known as Nervecentre. The Trust is in dialogue with Nervecentre as to potential options for functionality to be built into that system. However, any such functionality must be considered in the context of the requirement for medical records to be readily available for the safe and effective care of service users, both in planned and urgent care settings. When the Trust has identified the functionality that Nervecentre may be able to develop, then careful

consideration will be required on the part of the Trust Caldicott Guardian, Data Protection Officer, and Senior Information Risk Owner, in particular, as to the appropriateness of the implementation of such options.

30 In addition to systems functionality, the Trust has considered what additional improvements it can make and is currently working with its internal auditor, 360 Assurance, to conduct a survey exercise with a number of third-party NHS trusts to understand their approaches to the issue of potential unauthorised access to medical records. The Trust will consider the outcome of the survey when determining the appropriateness of any further steps it takes in this regard going forwards.

31 The Trust Data Protection Officer has identified concerns relating to potential unauthorised access to medical records. This is an issue that has been highlighted via bi-annual reports to the Trust Audit Committee since at least as early as 2023. Many of these incidents involved only a single individual accessing a single record, for example of a family member. However there have been instances of a more significant number of accesses to the records of service users in individual cases. Concerns had also been raised during 2022 in relation to unauthorised access to medical records in response to which the Trust ran a communications campaign at that time.

32 The Trust understands the importance of being clear with staff as to the legitimate access to medical records of service users. Various steps have been taken, particularly during the course of 2024, to improve awareness of data and confidentiality across the Trust. A further communications campaign has been developed which will run from July 2025 to May 2026, the outcome of which will be evaluated at the end of that period.

33 In conclusion, the Trust considers that its communication with the bereaved families and surviving victims has been appropriate once it became aware of concerns of potential unauthorised access to records. The Trust is determined to learn from experiences of this nature and is in the process of exploring any

further actions it can, or should, take going forwards to mitigate against such issues arising in the future. With regard to the staff members involved in the current matter, investigations are ongoing, and the Trust is committed to taking appropriate disciplinary and other action where this is determined to be appropriate.

THE TRUST

34 The Trust was established in 2006 and is the product of the merger between the former Nottingham City Hospital NHS Trust and the Queen's Medical Centre, Nottingham, University Hospital NHS Trust. This took place pursuant to the Nottingham University Hospitals National Health Service Trust (Establishment) and the Nottingham City Hospital National Health Service Trust and the Queen's Medical Centre, Nottingham, University Hospital National Health Service Trust (Dissolution) Order 2006 [NUHT0000069].

35 Across the Queen's Medical Centre, City Hospital and Ropewalk House sites the Trust has around 90 wards and 1,700 beds. It is one of the largest NHS Trusts in England responsible for delivering general services to around 2.5 million residents across Nottingham, Nottinghamshire and the surrounding area. The Trust also provides specialist services to up to 5 million patients from across the wider East Midlands, as well as various services at a national level. The Trust is a specialist centre for services including stroke, renal, neurosciences and cancer, as well as being home to the East Midlands Major Trauma Centre, the Nottingham Children's Hospital, and hosting the Biomedical Research Centre in partnership with the University of Nottingham.

36 The Trust employs circa 19,000 staff, being one of the largest employers across Nottinghamshire, with a further 750 volunteers.

37 With an annual budget of circa £1.9 billion the Trust is one of the biggest and busiest NHS trusts in the country.

RELEVANT LEGAL AND NATIONAL POLICY CONTEXT

38 The Trust operates within a structured legal context so far as the access to, handling and processing of patient medical records are concerned. The primary legal regimes are contained in data protection legislation and relevant case law establishing the common law duty of confidentiality. These legal obligations are supplemented by various policy documents including guidance and codes of practice, which further explain how those obligations are expected to be complied with in the context of the provision of healthcare.

39 It is helpful for the Inquiry to understand in broad terms the legal and policy context within which the Trust operates when considering the questions raised in the Rule 9 request of 3 June 2025, and so I have sought to summarise these here. In doing so I have not sought to set out a detailed legal analysis but to put into context the measures across the Trust which are relevant to the issue of unauthorised access to medical records.

UK General Data Protection Regulation ('UK GDPR') and the Data Protection Act 2018

40 The UK GDPR, as supplemented by the Data Protection Act 2018, sets out the legislative regime for the protection of personal data of living identifiable individuals in the United Kingdom, and is applicable to all processing of personal data by the Trust. The Trust is a data controller in respect of data that it holds relating to the treatment of patients under its care and the Trust must comply with its obligations in that role. Much of the data held on patients comprises health data/special category data. Patient data are accessed and used where it is necessary to do so, both for clinical care and secondary purposes such as audit and service improvement.

41 Article 5 of the UK GDPR sets out a number of data protection principles, which include that personal data be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using

appropriate technical or organisational measures. This principle is supplemented in particular by Article 32 of the UK GDPR which provides that a data controller must implement appropriate technical and organisational measures appropriate to the risk, and in doing so should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

42 In the following sections of this statement, I will seek to explain the technical and organisational measures in place within the Trust, focusing specifically on the issue of the access to patient records without a legitimate need.

Duty of Confidentiality

43 Distinct from the statutory data protection regime is the common law duty of confidentiality. The duty arises where information is disclosed in circumstances where the individual disclosing the information expects that it will remain confidential. It is generally accepted that information collected in the course of providing health and care services will be treated as confidential, until it is either no longer in an identifiable form or a lawful basis for overriding the duty of confidentiality applies.

44 The duty of confidentiality may be overridden only in certain specified circumstances, namely where the sharing of information is considered to be in the public interest, consent has been given or implied, and/or statutory provisions either require or allow such sharing.

45 Generally explicit consent is required to override a duty of confidentiality; however it is accepted that in relation to the provision of direct care, consent can be implied.

46 Unlike the statutory data protection regime which applies only to living identifiable individuals, the duty of confidentiality continues to apply to a

deceased person with an ethical obligation owed to the relatives of the deceased.

47 In practice this requires the Trust to take appropriate steps in order to ensure that confidential patient information is not inadvertently disclosed or otherwise accessed without a legitimate purpose.

48 By way of example, one particular area where the duty of confidentiality can be set aside is pursuant to Section 251 of the National Health Service Act 2006. This provides the Secretary of State with authority to make regulations that set aside the duty of confidentiality, for example for the purpose of enabling contact to be made with individuals to gain consent for research, or for clinical audit purposes. There are specific processes that must be followed prior to the making of such regulations including making an application to the Confidentiality Advisory Group. This is a body hosted by the Health Advisory Authority and which is consulted by the Secretary of State in making decisions as to whether to exercise discretion to make a regulation enabling the sharing of information for a particular purpose.

National guidance and policy in relation to the duty of confidentiality

49 The Department of Health and Social Care ('DHSC') has published a Confidentiality Code of Practice [NUHT0000016] and supplementary guidance [NUHT0000028], which was implemented in November 2003 and is intended to be a guide to required practice for those working within NHS bodies. It also has an Information Security Management NHS Code of Practice [NUHT0000049] which is a guide to the required methods and standards of practice in the management of information security.

50 NHS Digital, now part of NHS England, provides a resource on codes of practice for handling information in health and care. It sets out what health and care organisations must do to look after information properly, addressing confidentiality, information security management and NHS records

management. This confirms that the duty to share information can be as important as the duty to protect confidentiality.

51 The Health and Social Care Information Centre (renamed NHS Digital in July 2016) Guide to Confidentiality 2013 (updated March 2022) [WITN0226004] shows health and care workers how to share information safely while following confidentiality rules. The guide has been issued under powers to provide advice and guidance on any matter relating to the collection or dissemination of information. Health and social care bodies processing confidential information in relation to the provision of publicly funded health or adult social care activities, must have regard to this guide.

52 The confidentiality rules are:

a) Confidential information about service users or patients should be treated confidentially and respectfully.

b) Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.

c) Information that is shared for the benefit of the community should be anonymised.

d) An individual's right to object to the sharing of confidential information about them should be respected.

e) Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

53 It emphasises that confidentiality has been a cornerstone of medical practice for centuries, and the relationship of trust between a doctor and patients depend upon it, however it is also necessary for such confidential information to be shared in order to provide a seamless, integrated service.

What professional regulatory bodies say

54 Guidance is provided to clinicians by their relevant regulatory bodies. There are a number health and social care regulators which oversee one or more of the health and social care professions by regulating individual professionals across the UK. They include the General Medical Council ('GMC') (which regulates doctors), the Nursing and Midwifery Council ('NMC') (which regulates nurses and midwives), and the Health and Care Professions Council ('HCPC') (which regulates a wide range of professionals including dieticians, occupational therapists, paramedics and so on).

55 These regulators maintain guidance that regulated professionals are expected to comply with, including in relation to confidentiality and access to/disclosure of patient information. Each of these forms of guidance emphasise the importance of respecting confidentiality, appropriate information sharing and ensuring people are informed about how and why information is shared.

56 Guidance to all professionals emphasises the ethical and legal duties to protect information from improper disclosure, but significantly also that appropriate information sharing is essential to the provision of safe and effective care and that it is necessary for those providing care to have access to up to date and accurate information about patients to avoid them being put at risk.

57 For instance, the General Medical Council's guidance document 'Confidentiality: Good Practice in Handling Patient Information' [NUHT0000044 which all doctors must follow states:

> *"Trust is an essential part of the relationship between patients and medical professionals and confidentiality is central to this… Medical professionals are under both ethical and legal duties to protect patients' personal information from improper disclosure. But appropriate information sharing is an essential part of the provision of safe and effective care. Patients may be put at risk if those*

who are providing their care do not have access to relevant, accurate and up-to-date information about them.

There are also important uses of patient information for purposes other than direct care. Some of these are indirectly related to patient care in that they enable health services to function efficiently and safely… Other uses are not directly related to the provision of healthcare but serve wider public interests, such as disclosures for public protection reasons."

58 Guidance from the General Medical Council also specifically sets out that a doctor "must not access a patient's personal information unless [they] have a legitimate reason to view it" (see paragraph 120 of "Confidentiality: Good Practice in Handling Patient Information" [NUHT0000044]).

59 More widely all doctors are subject to the code of practice contained in "Good Medical Practice" [NUHT0000045], and which requires that all doctors must make sure that their conduct justifies patients' trust in them and the public's trust in the profession (see paragraph 81 of Good Medical Practice).

60 The Nursing & Midwifery Council confirms in their code of practice 'The Code: Professional standards of practice and behaviour for nurses, midwives and nursing associates' ('the NMC Code') [NUHT0000058]:

"As a nurse, midwife or nursing associate, you owe a duty of confidentiality to all those who are receiving care. This includes making sure that they are informed about their care and that information about them is shared appropriately."

61 The NMC Code confirms that those regulated by the Nursing & Midwifery Council "must respect a person's right to privacy in all aspects of their care."

62 Similarly, the HCPC 'Guidance on Confidentiality' [NUHT0000017] states that:

> *"[…] accessing information (including care records) without good reason, permission or authorisation is considered to be breaking confidentiality, even if you do not then share the information with a third party. You should be sure that you have a legitimate reason for accessing information about service users, for example where you need it to provide care, treatment or other services. For other reasons you are likely to need specific permission from the service user."*

63 Clinical staff are accountable to their relevant regulator who seek to ensure that professionals continue to maintain fitness to practise. Regulators are able to investigate concerns, and take action to address any concerns, including to issue warnings, or impose a sanction, including taking steps towards restricting, suspending or revoking registration where they consider appropriate.

64 The Medical Profession (Responsible Officer) Regulations 2010, as amended, require NHS trusts, and other designated bodies to appoint a Responsible Officer, who is accountable for the local clinical governance processes, with a focus on the conduct and performance of doctors, and where appropriate can require concerns to be referred to the General Medical Council.

The relevance of Caldicott

65 In 1997 the Caldicott Committee's Report on the Review of Patient-Identifiable Information [NUHT0000029] recommended six good practice principles to be applied to the use of confidential information in the health service. These became known as the Caldicott principles. These principles have become well established since then. Since 1998 each NHS body has been required to have a Caldicott Guardian, who is a senior person within that organisation responsible for the safeguarding of confidential patient information. The

appointment of a Caldicott Guardian is a specific requirement of the NHS Standard Contract (GC21) [NUHT0000002].

66 In 2013 the 'The Information Governance Review' [NUHT0000010] was published, reaffirming the Caldicott principles and recognising the value of the Caldicott guardian role. The purpose of this review was to seek to understand the appropriate balance between protecting patient information and the sharing of information to improve patient care. This review introduced a new Caldicott Principle which was intended to encourage information sharing in the best interests of patients, referring to a "culture of anxiety" around information sharing. This is the principle that:

> *The duty to share information can be as important as the duty to protect patient confidentiality.*

67 This principle is consistent with the guidance issued by professional regulatory bodies, and which recognise the importance of information sharing, and the availability of information for the purpose of the safe and effective delivery of care and treatment to service users.

The role of the National Data Guardian

68 The National Data Guardian ('NDG') was created in 2014 in order to champion the rights of patients and the public in relation to the confidentiality of their health and care information. The statutory office of the NDG was established by the Health and Social Care (National Data Guardian) Act 2018 ('the 2018 Act'), with the purpose of providing advice and guidance about the processing of health and social care data in England. The NDG may issue guidance, which all bodies in the scope of the 2018 Act must have regard to.

69 The NDG emphasises the need for improving the availability of information for direct care. In their most recent annual report published in December 2024 in respect of the period 2023/2024 [NUHT0000054] the NDG stated that "*[p]atients are often let down when they arrive for care and their clinician lacks*

information about important diagnoses or treatments received in other settings" and referred to the need for the NHS *"to ensure seamless and consistent access to the necessary patient data in each care setting. A strong foundation of effective information sharing is essential for improving patient outcomes and will provide a solid base for more advanced initiatives to build upon"*.

70 In 2020 the NDG carried out a survey to understand the barriers to sharing for direct care purposes, concluding [NUHT0000055]:

> *Modern health and care provision increasingly depends upon effective communication between professionals, patients, service-users and carers across different organisations and at multiple points in a person's interaction with the system. While the UK legal framework governing the sharing of data does allow health and care data to be used and shared for these purposes, the responses provided to this survey indicate that those working in the system feel that the law is so complex, poorly understood and difficult to navigate that they do not have confidence to do so.*
>
> *In this survey, we have heard clearly that patients may be suffering as a result. Relevant information about them is not being shared appropriately and not being made available at the point of care. Respondents to this survey also highlighted how, with the further blurring of boundaries between clinical and non-clinical elements of teams supporting people (through activity such as population health management), this environment is becoming ever more complex and the need for clear guidance and support in this area will only grow.*

71 The stance of the NDG provides important context to this matter from the perspective of the Trust, which must ensure the appropriate availability of patient data and access to patient records so as to be able to provide clinically safe and effective care.

The Data Security and Protection Toolkit ('DSPT')

72 The DSPT is an NHS online self-assessment tool that all organisations must use if they have access to NHS patient data and systems. It is intended to provide assurance that these organisations are practising good data security and handling of personal information properly. This is an annual requirement that must be completed by all such organisations, including the Trust. It measures performance against the ten data security standards introduced by the NDG in 2016 following their "Review of Data Security, Consent and Opt-Outs" [NUHT0000027]. Those security standards of particular relevance to the current matter are:

> *1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.*
>
> *2. 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.*
>
> *3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit*
>
> *4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon*

as it is no longer required. All access data to personal confidential data on IT systems can be attributed to individuals.

The Duty of Candour

73 The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 ('the 2014 Regulations') require at Regulation 20 that registered persons must act in an open and transparent way with relevant persons (either a service user or person acting on their behalf on the death of a service user) in relation to care and treatment provided to service users in carrying out a regulated activity.

74 The duty requires that as soon as reasonably practicable after becoming aware that a notifiable safety incident (one which is unintended or unexpected, has occurred during provision of a regulated activity, and in the reasonable opinion of a healthcare professional already has or might result in death or severe or moderate harm to the person receiving care) has occurred, a registered person must notify the relevant person that the incident has occurred, and provide reasonable support to the relevant person in relation to the incident, including when giving the notification. A fundamental element of the duty of candour is for an organisation to provide a timely apology for the incident, regardless of fault.

75 The duty of candour was introduced as a legislative requirement following findings of the Francis Inquiry as to serious failings in openness and transparency at Mid Staffordshire NHS Foundation Trust [NUHT 0000003]:

"The way in which the Trust handled the matter can be viewed as an object lesson in how the tragedy of an avoidable death can be exacerbated by inappropriate handling of the case. It demonstrates the sad fact that, for all the fine words printed and spoken about candour, and willingness to remedy wrongs, there lurks within the system an institutional instinct which, under pressure, will

prefer concealment, formulaic responses and avoidance of public criticism."

76 Guidance from the Care Quality Commission refers to the duty of candour as being "seen as a crucial, underpinning aspect of a safe, open and transparent culture" [NUHT0000013].

Care Quality Commission

77 In line with its purpose to ensure care services provide people with safe and effective care, the CQC also has powers to inspect the Trust's information governance as part of its inspection process. This comes under well-led key line of enquiry W6, "Is appropriate and accurate information being effectively processed, challenged and acted on?". [NUHT0000004]

78 The CQC specifically requires that medical records are accurate, fit for purpose, held securely and confidentially.

79 The CQC also assess whether there are measures in place to ensure the availability, integrity and confidentiality of identifiable data, records and data management systems, in line with data security standards, and whether lessons are learned when there are data security breaches.

Potential consequences when records are accessed inappropriately

80 In addition to the regulatory action that may be taken by professional regulatory bodies in relation to regulated individuals (doctors, nurses, midwives and others as referred to above), access to medical records without a legitimate purpose can result in criminal prosecution.

81 The Information Commissioner's Office has the power to prosecute individuals under Section 170 of the Data Protection Act 2018 for unlawfully obtaining personal data. In addition, the Computer Misuse Act 1990 contains various offences related to the unauthorised access to information on a computer, as well as for the unauthorised modification of data from a computer.

HOW THE TRUST SEEKS TO ENSURE COMPLIANCE

82 There is important context that must be understood when considering the role of the Trust in relation to the safe handling of patient data, particularly in the context of the provision of effective care and treatment to individuals in a hospital setting, and which is explicitly recognised in the national policy and regulatory position explained above.

83 The need to ensure confidentiality must always be considered against the inherent and important requirement to ensure that access to records is maintained to enable the safe and effective delivery of care. This is recognised in the policies and procedures of the Trust as well as the nature of the systems and access controls in place – namely the technical and organisational measures that have been adopted by the Trust.

84 It is important at this point that the Inquiry understands that the Trust did not initially take any specific steps in relation to the information generated as a result of the Incident with a view to ensuring that it was accessed only by those with a legitimate need for access. Instead, the Trust relied upon the existing processes, procedures and systems controls that it has in place generally in relation to the access to patient records, and that are described further below. These processes, procedures and systems facilitated an appropriate response to the matter when concerns were identified.

Policies, processes and procedures

85 The Trust has in place a number of policies, procedures and guidelines in relation to information governance. These are in place to support the Trust's overall strategy and promote a culture of good practice around the processing of information and use of information systems to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The Trust requires all employees to comply with its policies, procedures and guidelines.

86 The Trust has a scheme of information governance and disciplinary policies in place, as required under the statutory and mandated scheme set out above. I have set out below the relevant policies which were in place at the time of the Incident, and the policies which employees were expected to comply with at the time of accessing the data. In addition to this, I have also set out the policies that the Trust now has in place, to which employees are currently subject, and under which the Trust's investigations are proceeding.

Policy position at the time of the incident

87 At the time of the Incident, the Trust had in place an Information Governance Management Framework (GG/INF/017) [NUHT0000034], which incorporated its Information Governance Policy. As of 3 April 2023, version 5 of this framework was in place. It included information around the National Data Security Standards, Data Security and Protection Toolkit, and relevant standards and responsibilities.

88 This framework set out the Data Security Standards as discussed above at 88and reiterates that the Trust would ensure the confidentiality of personal information, and that all staff must ensure that personal confidential data is handled, stored and transmitted securely. It also stated that all staff must understand their responsibilities and obligations, including their personal accountability for deliberate or avoidable breaches, and that the Trust would ensure that all clinical and corporate records were managed in accordance with mandated and statutory requirements.

89 The Trust also had in place a Data Protection, Confidentiality and Disclosure Policy (GG/INF/026) [NUHT0000026], which was in place to inform staff of their legal duties around confidentiality, provide guidance on keeping personal information secure and confidential, and to make staff aware of the correct procedures for disclosing personal information.

90 This policy set out the consequences for policy breaches, including that all Trust employees and anyone else working for the Trust must understand their responsibilities for data protection and confidentiality.

91 It made clear that breaches of confidentiality without justifiable reason may constitute gross misconduct and may result in dismissal even for a first offence.

92 Finally, the Trust had in place the Conduct, Behaviour and Disciplinary Policy and Procedure (HR/P&C/017) [NUHT0000060] implemented on 2 May 2023, the Conduct, Capability and Ill Health Procedure for Medical Practitioners (HR/P&C/016) [NUHT000015] implemented on 9 February 2023, and the Information Security and Risk Policy (GG/INF/002) [NUHT0000031] implemented on 31 March 2022. These policies are still in place. The Conduct Policies are discussed further in relation to HR processes and investigations below at 121- 131, and the Information Security and Risk Policy is discussed below at 105 – 107.

Current Policy Position

93 Since 11 December 2024, the Trust has had in place its Information Governance Management Framework (GG/INF/035b) ('IGMF') [NUHT0000050], which replaces the Trust's Information Governance Management Framework (GG/INF/017). The purpose of the IGMF is to describe the management arrangements that deliver information governance assurance across the Trust.

94 The Trust's intention was to create an Information Security Management Framework ('ISMF') to sit alongside the current IGMF. At the time of producing this statement this has not been developed, and the relevant current policy position remains the Trust's Information Security & Risk Policy [NUHT0000031].

95 The Trust approach to information governance is in setting a high standard for the handling of information and ensuring the Trust and its staff have the tools

to achieve that standard. The aim is to demonstrate that the Trust can be trusted to maintain the confidentiality and security of personal information, by helping individuals to practice good information governance and be consistent in the way it handles both personal and corporate information. The six core policies within this framework, and which are explained at a high level below, are the:

a) Information Governance Policy [[NUHT0000043]

b) Data Protection Policy [NUHT0000042]

c) Confidentiality Policy [NUHT0000041]

d) Information Security and Risk Policy [NUHT0000031]

e) Records Management Policy [NUHT0000032 and NUHT0000033]]

f) Social media [NUHT0000030]]

Information Governance Policy

96 Following consultation with the Data Protection & Cyber Security Panel Members, Information Asset Owners, and Digital and Data Strategic Committee, a new Information Governance Policy (GC/INF/035a) [NUHT0000043] was approved by the Trust Board and implemented on 11 December 2024. The policy is scheduled for review in December 2027. Alongside the IGMF, it replaces GG/INF/017, the previous Information Governance Management Framework [NUHT0000034].

97 This policy provides guidance to all staff on information governance, in particular how to look after information that they need to do their jobs and how to protect this information on behalf of service users and staff. It is intended to provide a consistent way for employees and others, including contractors, and agency employees to deal with the information handling requirements in place at the Trust.

98 The Policy sets out the roles and responsibilities of various Trust Committees and Officers and outlines the information governance processes to support implementation of the legal framework and applicable policies and codes of practice. For instance, the policy sets out the NDG Data Security Principles and the requirements for the Trust to adopt these, as discussed above at paragraphs 68 - 71.

Data Protection Policy

99 The Data Protection Policy (GG/INF/034) [NUHT0000042] was, following consultation and completion of an Equality Impact Assessment, implemented on 14 November 2024, alongside the Confidentiality Policy it replaces the previous Data Protection, Confidentiality & Disclosure Policy (GG/INF/026).

100 This policy recognises the need of the Trust to collect personal information about people with whom it deals, including patients, in order to carry out its business and provide its services. This includes private and confidential information. Regardless of the way by which data is collected, recorded and used this personal information must be dealt with appropriately to ensure compliance with the relevant legal framework.

101 The policy provides that the Trust will ensure compliance with the Data Protection legislation, as discussed above at paragraphs 38 - 48. It states that the Trust take a privacy by design approach and that the Trust employees are responsible for ensuring they use personal data appropriately and that they comply with data protection legislation.

Confidentiality Policy

102 The Confidentiality Policy (GG/INF/033) [NUHT0000041] was introduced alongside the Data Protection policy on 14 November 2024.

103 This policy sets expected commitments to the confidentiality of client and employee information and the Trust's responsibilities regarding the disclosure

of such information. It incorporates the responsibilities of employees to ensure confidentiality with regards to any sensitive information. All employees working with partner organisations are bound by a legal duty of confidence to protect personal information they come into contact with during the course of their work.

104 The policy is also to ensure employees are aware of the correct procedures for maintaining confidentiality of client information so that they do not intentionally or inadvertently breach any requirements of law or good practice.

Information Security Policy

105 The current version, version 6, of the Information Security and Risk Policy (GG/INF/002) [NUHT0000031] was implemented on 31 March 2022. It superseded version 5, from August 2020. The policy was due for review in March 2025, and at the time of submitting this statement work is underway to progress a review.

106 This policy recognises that information has the greatest value when accurate, up to date and accessible where needed. It confirms that effective security management is underpinned by robust risk management processes which require the Trust to have a structure in place which reduces risks and threats to information whilst retaining security, availability and accessibility.

107 The policy provides that the Trust has a responsibility to maintain confidentiality which confirms that "[a]access to data must be confined to those with specific authority to view the data.", and also that the Trust must maintain availability, in that "[I]nformation must be available and delivered to the right person, at the time when it is needed".

Records Management Policy

108 There are policies which apply to both healthcare records, the Health Records Management Policy (GG/INF/006) [NUHT0000032] and non-care records, the Corporate Records Management Policy (GG/INF/023) [NUHT0000033].

109 The Corporate Records Management Policy currently in place is version 4, and was implemented on 12 December 2020, superseding a version from April 2015. The Health Records Management Policy is currently on version 6, which was implemented in March 2023. Both policies are currently due for review.

110 Records Management is the process by which an organisation manages all aspects of records however generated, and regardless of format or type, throughout their lifecycle. The Records Management: NHS Code of Practice [NUHT 0000057], published by the Department of Health and Social Care, details the required standards of practice for those working within NHS organisations in England in the management of records.

Social Media Policy

111 For completeness, the final of the six policies under the IGMF is the social media Policy [NUHT0000030]. Version 4 of the policy (GG/CM/053) was implemented on 25 April 2023. This policy aims to ensure that all employees across the organisation enjoy the benefits of social media, whilst understanding their obligations and responsibilities to their employer, partners, colleagues, service users and carers.

Contractual obligations, training and communications

112 The Trust has a Mandatory Training Policy [NUHT0000047] which sets out the Trust's arrangements for mandatory training, as defined by the NHS Core Skills Training Framework [NUHT0000025] as well as those identified through internal governance and training needs analysis. The Trust also has a Temporary Staffing Policy [NUHT0000046] which covers temporary staff working less than 8 weeks, or locum staff.

113 The DSPT (explained above at paragraph 72) mandates that employees receive training in information governance and data security. Employees of the Trust are required to complete a Data Security Awareness course, in order to be compliant with the Trust's Mandatory Training Policy.

114 The training Trust employees are mandated to undertake is the national NHS Digital Data Security Awareness training course [NUHT0000056], which is developed by NHS Digital and is considered to meet the statutory and mandatory training requirements and learning outcomes for information governance set out under the UK Core Skills Training Framework (a national minimum standard for statutory and mandatory training in the health sector) set by Skills for Health which are as follows:

a) understand the principles of Information Governance and the importance of data security in health and care

b) understand the different types and value of information

c) understand the principles of data security, including how to ensure the confidentiality, integrity and availability of data

d) be aware of threats to data security and know how to avoid them, including:

   i. Social engineering

   ii. Using social media safely

   iii. Using email safely

   iv. Malicious software

   v. How to protect information

   vi. Physical security

e) be able to identify data breaches and incidents and know what to report

f) understand fundamentals of data protection and the General Data Protection Regulations (GDPR)

g) understand the Caldicott Principles and be able to provide a confidential service to patients and service users

h) understand the responsibilities of healthcare organisations under the Freedom of Information Act 2000

i) understand individual responsibilities in responding to a Freedom of Information request

115 The Trust has predominantly used the national training course referred to above as its information governance training since March 2021. The current version was updated in February 2025. Between March 2021 and April 2022, the Trust also used an additional local training video but this has not been in use since April 2022 [WITN0226002A] [WITN0226002B]. A proposed potential new approach to Data Protection and Security Training [NUHT0000009] is also currently under consideration within the Trust.

116 Alongside annual mandatory training, materials are issued to individuals with IT accounts when they join the Trust. This includes a key information sheet for new starters as part of their employment pack, providing an introduction in relation to *Information Governance and Data Protection at NUH* [NUHT0000048] from April 2022, superseded by [NUHT0000008] in August 2024 but retaining the following wording. This key information sheet states in order to ensure good information governance, in relation to system access:

> *"ONLY access/view personal information within systems/records you have access to, if you have a legitimate work-related reason to do so, e.g. direct care.*
>
> *a. You MUST NOT access your own records, families, friends, colleagues etc…*
>
> *b. Any suspected breach will be investigated and reported to HR and could result in dismissal and referral to*

regulatory bodies, Police, and ultimately result in a criminal record!"

117 There is currently also a welcome from the Data Protection Officer on the Trust intranet which is issued to new starters with account details [NUHT0000051].

Employment Contracts and Conditions

118 The Trust's employment contracts contain provisions relating to confidentiality of information. Staff are required as part of their employment contracts to comply with the policies and procedures for acceptable use and access of systems and maintaining confidentiality at all times.

119 The Trust have a range of template employment contracts which are largely divided between medical professionals and Agenda for Change staff. Agenda for Change staff are all staff except doctors, dentists, and very senior managers. The Trust's contracts include:

a) AfC Apprentice Contract [NUHT0000011],

b) AfC General Contract [NUHT0000012],

c) Medical Consultant Contract [NUHT0000052],

d) Medical Locum Consultant Contract [NUHT0000053],

e) Resident Doctor Contract [NUHT0000059],

f) Specialist Grade Contract [NUHT0000061],

g) Specialty Doctor Contract [NUHT0000062],

h) Trust Grade Doctor Contract [NUHT0000068].

120 These contracts either contain explicit provisions relating to the issue of confidentiality, and/or incorporate national Terms and Conditions produced by NHS Employers which impose obligations relating to confidentiality. Whether

via explicit provisions directly in these contracts or by reference to standard Terms and Conditions, all staff of the Trust are subject to contractual requirements relating to maintaining confidentiality of patient information.

Relevant Incident Management and Human Resources Policies and Procedures

121 The Trust's Conduct, Behaviour and Disciplinary Policy and Procedure (HR/P&C/017) [NUHT0000060] implemented on 2 May 2023 is in place to ensure a fair, systematic and consistent approach where the behaviour or conduct of a member of staff breaches workplace rules or standards. All employees have personal duties to ensure their compliance with relevant conduct and behavioural requirements.

122 This policy confirms that a breach of confidentiality, or misuse of authorised access to information and systems, unauthorised access to information and systems, and any activity that could breach the security of Trust information and technology infrastructure or any other breach of Trust information security policies can constitute misconduct.

123 The policy also confirms that gross misconduct can include a serious breach of the Trust information security policies including serious misuse of authorised access/unauthorised access to information and systems, as well as unauthorised access to, use or disclosure of confidential information including the unauthorised use or disclosure of any computer-held or computer-generated information,

124 The Trust has reporting procedures for investigation of data breaches and data breach allegations which should be escalated immediately to senior managers, a member of the information governance team and a member of the human resources team.

125 The Trust has an Information Governance and Digital Services Security Incident Management Procedure for Personal Data Breaches [NUHT0000006]. This was implemented in March 2020. It provides guidance for handling

incidents resulting in personal data breaches including unauthorised/inappropriate access to personal data.

126 Where there are allegations of potential misconduct and gross misconduct, for all registered medical staff employed by the Trust, including doctors and dentists in training, the Conduct Capability and Ill Health Procedure for Medical Practitioners [NUHT0000015] applies. The policy includes the appropriate processes to be undertaken in the case of alleged misconduct, as well as possible steps that should be taken. This can include onward communication to other bodies such as other organisations where the individual may work or the appropriate professional body such as the GMC, it can also include revoking digital access where there are concerns about inappropriate record access.

127 For all other staff, misconduct is dealt with under the Conduct, Behaviour and Disciplinary Policy and Procedure [NUHT0000060]. Under this policy, alleged incidents will be carefully assessed. Initially a fact-finding exercise is undertaken by a line manager to establish the employee's version of events and the context around the issue. This can involve meetings with other relevant individuals. Potential outcomes include informal action, further training, an agreed outcome or formal investigation.

128 Where further investigation is required and/or formal action, this must be approved by a commissioning manager who will provide independent oversight. Terms of Reference will be produced and can be commented upon by the employee.

129 The investigation can result in a formal conduct and behaviour hearing. The Trust's policy sets out the processes that are to be followed around this.

130 The information governance team have oversight for all information governance breaches and must be kept informed.

131 The Trust also has an investigation checklist, which sets out how investigations are carried out, how severity can be assessed and how employees will be dealt

with in relation to breaches. It also details the duties to onward report to the data subject, professional regulatory bodies and others.

132 Within the checklist, a minor breach example given is looking at your own records or that of a close family member to check if an appointment has been made. The suggested outcome is that the employee must re-take Information governance training, and a conversation must take place to record the situation and express the severity of the incident, and the potential consequences of a repeat. This will be followed up in writing and placed on the employees file [NUHT0000007].

133 The Trust is subject to the Duty of Candour, as discussed above at paragraphs 73 to 76. Separately, the Trust must make an informed decision in individual cases of data breaches as to whether to notify those whose data has been compromised as well as whether reporting is required to the Information Commissioner's Office. Data subjects should be kept informed of the stage and final outcome of an investigation in serious cases where there is a risk to that data subject or possibly where the case has arisen out of a complaint.

134 It is also necessary in each case for the Trust to consider whether reporting to the police is appropriate where there has been a serious breach of the data protection legislation or Computer Misuse Act 1990 which has been reported to the Information Commissioner's Office, or whether in the case of regulated professionals, reporting to professional regulatory bodies would be appropriate or required. This can be done prior to the investigation concluding depending on the severity of the breach.

The core patient systems operated by the Trust

135 The Trust operates a number of systems in relation to the provision of care and treatment to patients. This is similar to the position of other NHS Trusts and NHS Foundation Trusts nationally, but there is no consistent position across all such organisations. Each organisation is responsible separately for commissioning the systems that it utilises locally, and the reasons for

commissioning certain systems may be influenced by a number of factors. The NHS does not have a single, national electronic system for Trusts to adopt. The selection and procurement of electronic patient records and associated systems is devolved to individual Trusts, though is increasingly co-ordinated within geographic areas. Factors that are taken into account in relation to selection of systems include range and depth of functionality, usability, decision support capabilities, security, interoperability with other systems, data analysis capabilities, clinical safety assessments and total cost of ownership.

136 The Trust uses Microsoft Windows as an operating system across all its sites. All staff accessing the system require a username and password to do so with appropriate mechanisms in place to lock a user account for a period of 15 minutes following three incorrect attempts at logging into the system. Upon logging on to the operating system all members of staff are presented with a warning relating to appropriate use. Staff are required to change passwords every six months, and those passwords must be a minimum of twelve characters, with it not being possible to use previous passwords. Screens will either lock or screensavers appear after specified periods of time. The Trust is considering whether additional security amendments are required to the current measures and timeframes within which these should take place.

137 The core patient systems in place across the Trust are explained below. For the purposes of this statement, I have sought to explain at a high level the purpose and function of each system, how access controls work within the system, and the audit functionality, as key aspects relevant to the issue of unauthorised access to records.

138 In respect of each of the systems referred to below, the Trust operates a role-based accessed controls scheme. This means that staff will have a different extent/level of access to the systems used by the Trust determined by that role's legitimate need for such access.

139 The access scheme is not patient-specific. If, for example, a clinician requires access to a patient's record, the clinician does not require a discrete authorisation for such access apart from the general access right based on their role. However, every access is logged and can be audited.

140 The nature of acute medicine means there is a high risk attached to restriction of records where many members of staff may require access to a record to treat the patient, sometimes in an emergency. However, members of staff are accountable for each access to a patient record, both to the Trust and, in the case of regulated professionals, to their professional bodies. The approach to accessing records in place at the time of the Incident reflected the Trust's attempt to balance patient confidentiality with the need to provide safe care, often under urgent and 'life and death' circumstances. Furthermore, even in planned care situations, it is not possible to pre-empt all members of staff who may require access to a patient's record as part of the administration or provision of that care.

141 A detailed spreadsheet has been produced by the Trust in support of its reporting requirements under the Data Security and Protection Toolkit annual self-assessment, and the supporting assessment of system level security for core Information and Communications Technology patient systems [NUHT0000063 and NUHT0000024]. This spreadsheet sets out the access level of different roles within the Trust, and the rationale for that level of access.

142 All of the core patient systems referred to below retain a complete record of all accesses to a patient record for audit purposes. Such audits can be conducted either by searching by reference to the name of a member of staff, or by the name of a patient. A "*Datix Audit Request – Systems Audit"* document has been produced by the Trust Application Management Team which explains the nature of and process for audits of each system [NUHT0000014]. All audits are conducted by the Trust Application Management Team, and other than the DHR system (explained further below), users are unable to generally see who else has accessed a record without an audit being requested from this team.

143 These audit capabilities facilitate the ability to conduct full audits in circumstances where there is considered to be potential unauthorised or illegitimate access to patient records, so as to facilitate investigatory and disciplinary processes by the Trust where appropriate.

144 Access to each of the systems referred to below is restricted to only those staff working in roles providing or supporting clinical care.

145 A document explaining the access permissions of the core patient systems relevant to the current matter has been produced and is exhibited with this statement to assist the Inquiry [NUHT0000018].

146 The core patient systems of the Trust and which are relevant to the current circumstances are as follows:

a) Careflow

This is currently the core patient administration system ('PAS') that is used across the Trust and is provided by the company 'System C'. Its purpose is to capture patient information and activity, and includes the following functionality:

- Retention of a Patient Master Index recording patient demographic details, hospital identifiers and a summary of patient activity
- Appointment scheduling for new and follow-up outpatient appointments
- Management of all elective care, planned and booked patient admissions
- Catering for admission, transfer and discharge of inpatients, and all associated enquiries

- Monitoring and maintenance of the Referral to Treatment target wait periods and linked patient pathways to seek to avoid breaches
- Electronic tracking of paper case notes locations
- Diagnosis and procedure coding recorded against outpatient and inpatient attendances
- Viewing and recording of patient activity in Emergency Department (this was the case at the time of the Incident, but has since moved to Nervecentre as part of the wider transfer of all PAS functions to Nervecentre)
- Viewing and creating clinical notes
- Managing electronic test orders
- Viewing test results

Access to Careflow requires inputting a username and password.

Two warnings appear to users when accessing Careflow. The first appears upon access to the relevant domain within the operating system. A pop-up appears at this point prior to details being entered to log on to the system warning the user that unauthorised access is not permitted, stating: "unauthorised access, disclosure or improper use of this system and data is strictly prohibited in line with the Data Protection Act 2018, Computer Misuse Act 1990, Caldicott Principles and may result in disciplinary action. Accessing the system to view, print or amend records relating to yourself or other patients not directly in your care is a breach of the above. All activity is auditable; by continuing to use this system, you agree to comply with these terms and conditions". Upon opening Careflow post login, a further warning message appears which states: "unauthorised attempts to access these systems will be

logged and may result in disciplinary procedure". Whilst these messages appear on accessing the Careflow system, no further messages appear upon access to an individual patient record.

b) Unity Digital Health Record ('DHR')

This system is the Trust's Electronic Document Management System and is used to view digitalised patient case notes across the Trust. It is hosted by the company Fortus. It provides functionality to enable digitised records to be located within the system by various means including via the Patient Master Index, searching by inpatient or outpatient appointments and admissions, and viewing documents by date scanned or ingested to the system.

Currently, and at the time of the incident, no warnings are presented either upon access to the system or when accessing individual patient records.

c) Nervecentre

This system is the Trust's point of care electronic record system, and is used to record electronic observations, bed management, complete assessments, and request portering across the Trust. It is provided by Nervecentre. This system captures patient information and activity, and its purpose and functionality include:

- Entering and viewing patient observations, and escalating to appropriate staff based on early warning scores
- Electronic handover
- Completing certain patient assessments (currently nursing assessments, dementia, confirmation of death and Coroner's screening)

- Assigning ward beds and enabling monitoring of ward bed capacity
- Making referrals to other teams, then triggering further actions
- Running reports on recorded activity
- Monitoring live patient flows by way of location and bed occupancy
- Raising portering referrals and enabling assignment of tasks in this regard
- Electronic prescribing of medicines across adult inpatient, maternity, critical care and emergency departments
- Capturing patient information and activity within the emergency care setting including pre-registering, admitting to the emergency department, transfers, and recording patient notes during an episode in the Emergency Department and when discharging
- Viewing results and ordering investigations for pathology and radiology patients in emergency care

Currently, and at the time of the incident, no warnings are presented either upon access to the system or when accessing individual patient records.

The Trust is in the process of replacing the PAS functions currently undertaken within Careflow by Nervecentre. Nervecentre has already taken over as the main system used in the Emergency Department and is due to replace Careflow Trust-wide from October 2025.

d) Notis

This system is a local developed in house IT system designed to provide a clinical desktop for Trust staff. It was primarily intended to be an interim solution to create a single electronic view of clinical record of the former Queen's Medical Centre NHS Trust and Nottingham City Hospital NHS Trust, which now form the Trust. This pre-dated the delivery of the single NHS wide Electronic Health Record. The purpose and functionality of this system include:

- Viewing a patient record, including demographic details and activity information relating to outpatient and inpatient attendances
- Recording discharge information from ward beds
- Viewing results for radiology

Currently, and at the time of the incident, no warnings are presented either upon access to the system or when accessing individual patient records.

e) Picture Archiving and Communication System (PACS)

This system is used to view and report upon diagnostic images (such as x-rays and CT, MRI and ultrasound scans) across the Trust, and facilitates the viewing of such images, production of reports in relation to those images, and for marking results or reports as critical. It is supplied by GE and provided by the East Midlands Radiology Consortium (a group of NHS bodies aimed at delivering timely and effective radiology services across the East Midlands).

Login details are the same as those for the operating system, with the same requirements applying as explained above.

Currently, and at the time of the incident, no warnings are presented either upon access to the system or when accessing individual patient records.

THE FACTUAL AND CHRONOLOGICAL POSITION

147 The Trust first became involved with the victims of Mr Calocane when they were admitted to the Queens Medical Centre Emergency Department on 13 June 2023. The period of involvement in respect of the deceased victims generated limited information following 13 June 2023. In respect of the surviving victims the period for which the Trust holds records for them is longer due to ongoing provision of treatment.

148 The Trust was not aware of inappropriate or unauthorised access to the medical records of either the deceased or living victims until October 2024.

Photographs and video footage

149 As part of the processes referred to below, the Trust has considered whether the information accessed without legitimate purpose contains any photographs or video footage. No photographs are contained in the records that have been accessed other than a single photograph of a bruise in the records of one of the victims, and the systems known to have been accessed do not have the ability to store videos. No such video information was therefore accessed.

150 The Trust has specifically considered the issue of CCTV footage, including seeking to verify the position by way of an investigation conducted by independent Counsel in relation to the deceased victims and which is explained further below. In summary, all of records of the deceased victims have been checked and have been confirmed to contain no CCTV. The Trust does not retain CCTV within medical records, and I am not aware of any circumstance where this has happened. In addition, the Trust's CCTV systems retain recordings for a 31-day period and no footage which may have existed on arrival of the deceased individuals at Queens Medical Centre Emergency

Department was retained beyond this period. The Trust anticipates based on correspondence with the instructed Counsel to date, that the same position applies to CCTV footage that may have existed of the surviving victims on or around the time of the Incident.

Notification of Concerns to the Trust

151 On 4 October 2024, Nottinghamshire Healthcare NHS Foundation Trust submitted a request to the Trust, via their respective Data Protection Offices, for systems audit data following a request by the legal representatives of the families of the deceased victims. They sought to determine whether any individual employed by Nottinghamshire Healthcare NHS Foundation Trust had accessed the records of those victims. At this stage it was not, as far as the Trust was aware, in relation to a Trust employee accessing records of patients involved in the Incident. The request for information was guided by the knowledge that Nottinghamshire Healthcare NHS Foundation Trust had a team of staff who worked within the Trust's Emergency Department and who may have had access to the Trust's clinical systems within that role. The request specifically enquired as to whether any Nottinghamshire Healthcare NHS Foundation Trust staff had accessed those records. A case was opened on Datix which is the Trust wide incident reporting software used to log all incidents, including data breaches.

152 On 8 October 2024 further information was sought by the Trust Data Protection Office from Nottinghamshire Healthcare NHS Foundation Trust in relation to the request prior to proceeding to conduct the requested audit [NUHT0000070]. Additional explanation was provided on 10 October 2024 [NUHT0000071] and chased on 14 October 2024 [NUHT0000072]. On the same day, a copy of the request from the families and details of specific staff members against whom searches were sought was requested from Nottinghamshire Healthcare NHS Foundation Trust [NUHT0000073].

153 The response received on 16 October 2024 [NUHT0000074] indicated that the letter sent on behalf of the families did not list specific staff members and suggested that it may be appropriate therefore for the Trust to conduct audits on each patient to identify those individuals who had accessed their records as an alternative approach. The Trust responded on 17 October 2024 [NUHT0000078] asking that the families' legal team contact the Trust directly should such audit requests be required due to the Trust's role as data controller in respect of the information held. Following this, Nottinghamshire Healthcare NHS Foundation Trust referred to an information sharing agreement [NUHT0000076] between it and the Trust as the basis for the sharing of such information relating to individuals under its employment.

154 On 25 October 2024 Nottinghamshire Healthcare NHS Foundation Trust provided additional information which was considered by the Trust Data Protection Office to be sufficient to enable the case to be reopened. Systems audits were requested within the Trust on 6 November 2024. The relevant results were extracted and provided to Nottinghamshire Healthcare NHS Foundation Trust on 20 November 2024 [NUHT0000080]. The result indicated that no staff of Nottinghamshire Healthcare NHS Foundation Trust accessed records of the deceased victims. The Trust Data Protection Office requested in this correspondence that it be informed if the processes being undertaken by Nottinghamshire Healthcare NHS Foundation Trust identified any individuals employed by the Trust. The same day the Trust received a response stating that the audits did not reveal any access to records by staff of Nottinghamshire Healthcare NHS Foundation Trust [NUHT0000079]. The Trust Data Protection Office therefore closed the case on 29 November 2024.

155 On 9 December 2024 [NUHT0000081] the Data Protection Officer of Nottinghamshire Healthcare NHS Foundation Trust sent further correspondence to the Trust informing that following further detailed consideration they had identified a clinician who worked for both organisations and requested that checks be undertaken to determine whether or not their

access to the Trust's records was appropriate. The case was re-opened on the Datix system on 11 December 2024 as a result of this new information.

156 During the same period, the Trust Caldicott Guardian was contacted by the Medical Director of Nottinghamshire Healthcare NHS Foundation Trust, Dr Sue Elcock. On 23 December 2024 these individuals liaised in relation to what was considered to be a potential data breach by a doctor, but at this time no reference was made to this being related to the incident on 13 June 2023 or any other high-profile matter. The Caldicott Guardian made internal inquiries with the Trust Assistant Head of Medical Workforce and established that the doctor in question was working in the Trust at the time. This information was relayed by the Caldicott Guardian to Dr Sue Elcock on 24 December 2024.

157 At the same time, on 24 December 2024 the Trust Data Protection Office emailed the Data Protection Officer at Nottinghamshire Healthcare NHS Foundation Trust seeking specific details of the individual involved in respect of the enquiries made during October through to early December in order to enable the investigation to be progressed. The doctor's name was provided., At that stage it was unclear whether or not access to the records was legitimate, and further investigation was required [NUHT0000089].

158 During this period neither the Trust, nor Nottinghamshire Healthcare NHS Foundation Trust were aware of the other's investigations, nor that the enquiry from Dr Elcock was being made specifically in relation to the events of 13 June 2023.

159 During January 2025 the Data Protection Office of the Trust sought to establish internally where the doctor worked within the Trust. It was determined that they were "bank" staff (temporary staff that could be called upon to fulfil shifts) and as a result did not have a formal line manager within the Trust [NUHT0000090]. This was relevant as to any referral to, and investigation by, the Trust's human resources team. The Data Protection Office gave consideration as to how any investigation process might take place under these circumstances.

160 The parallel concern raised by Dr Elcock with the Caldicott Guardian also continued separately during this period. On 20 January 2025 Dr Elcock contacted the Trust Assistant Head of Medical Workforce seeking further assistance to investigate whether the doctor under consideration would have had grounds to access records. The Trust Assistant Head of Medical Workforce referred the matter to Dr Nav Bhandal, Deputy Medical Director for Professional Standards, and Myles Timson for assistance. Dr Bhandal has worked for the Trust for several years, is well known within the Trust, and is often the first point of contact for concerns related to doctors.

161 On 4 February 2025 Dr Elcock raised this matter directly with me. I contacted Dr Bhandal on 5 February 2025 seeking assistance, and she responded with information about the doctor in question the same day. Dr Bhandal sought assistance from the Caldicott Guardian to obtain audit trails in respect of access to the three deceased victims records. The audit reports were provided by the Trust's Digital Services team on 10 February 2025. The Caldicott Guardian provided the audit reports to Dr Bhandal on 11 February 2025 indicating that the records were accessed by the doctor in question.

162 Dr Bhandal proceeded to obtain information in relation to the doctor in question, and their placements within the Trust. This exercise confirmed that on 13 June 2023 they were doing a "taster day" within the Trust ophthalmology department. The audit records indicated there had been access to all three deceased victims' records on 19 June 2023, during which time the doctor was working on a night shift in the Trust acute medicine department.

163 Dr Bhandal discussed the matter with me on the same day. I then discussed the matter with the Caldicott Guardian who agreed to conduct an initial screening of the audit reports for all three deceased victims to identify any wider access to these records that might potentially be of concern. It was agreed that the Caldicott Guardian would contact me to confirm their findings.

Initial identification of concerns and first steps

164 On 12 February 2025 the Caldicott Guardian conducted their initial screening exercise as agreed. This exercise involved conducting an initial review of the Careflow system audit data and forming an initial view based on whether the individual accessing the records was likely to have legitimately been involved in the direct care of the individual concerned. The Caldicott Guardian determined based on their initial screening review that a full human resources investigation would be required in relation to potential unauthorised access to the records of the three deceased victims. An in-depth audit trail on the Trust's relevant core systems began to enable further investigation.

165 The Caldicott Guardian logged a new Datix record following his concerns. It was later identified the new Datix related to a previous Datix pertaining to the same issue, raised via both organisations' respective data protection teams. A decision was made to continue to investigate the matter pursuant to the concern raised directly with the Caldicott Guardian, but with a broader remit.

166 I was informed of the position by the Caldicott Guardian on 12 February 2025 and on the same day updated Anthony May (Chief Executive), Tracy Pilcher (Chief Nurse and Deputy CEO) and Jack Adlam (Director of Communications and Engagement).

167 The Caldicott Guardian reported the incident as a potential data breach via the Data Security and Protection Toolkit on 12 February 2025 [NUHT0000092]. The report to the Information Commissioner's Office stated that the initial review of audit data by the Caldicott Guardian indicated in the order of 20 to 30 likely inappropriate access events. The report indicated that further investigation was required with relevant individuals to determine whether there was a legitimate reason for access to the records. The report was allocated incident reference 41136.

168 On 12 February 2025 the Caldicott Guardian notified the Data Protection Officer and Senior Information Risk Officer of his reporting of the matter to the

Information Commissioner's Office. The Caldicott Guardian advised that they had conducted an initial review of audit trails in respect of the patient records and that it was apparent that there would be many episodes of inappropriate access, requiring a full incident management handling process.

169 In accordance with usual practice, the Trust Data Protection Office also informed the Chief Executive, Anthony May, of the incident on 13 February 2025 in his capacity as Accountable Officer [NUHT0000091]. A meeting between members of the Trust Executive Team and the Caldicott Guardian was convened on 13 February 2025, where an Incident Command Group was established to meet on a regular basis in respect of this incident. The Incident Command Group initially met twice daily, with these taking place less frequently as the matter progressed and as various actions were completed. The first meeting took place on 13 February 2025. I exhibit with this statement a bundle of the logs from meetings of the Incident Command Group from 13 February 2025 to 8 July 2025 [NUHT0000145], and which record the decision making of the Incident Command Group.

170 The matter was referred to the human resources team the same day for formal investigation and potential disciplinary processes, attaching initial spreadsheet audit trails from the Careflow and DHR systems [NUHT0000147]. Data from Nervecentre followed after this and once the request for detailed audit information had been received from colleagues within the Trust responsible for conducting audits of records.

171 The Caldicott Guardian produced a briefing note recording the timeline of events and agreed actions, which was subsequently updated on 17 February 2025 [NUHT0000136], and which has informed the timeline that I have set out above. A briefing note was also produced by the Data Protection Officer on 17 February 2025 [NUHT0000135].

172 On 14 February 2025 members of the Trust human resources department met and agreed a process to investigate any potential unauthorised access to

medical records of the deceased individuals. A multi-disciplinary Task and Finish Group ("the Group") was established, comprising Dr Jeremy Lewis (Caldicott Guardian), Dr Nav Bhandal (Deputy Medical Director – Professional Standards), Dr Nuhu Osman (Deputy Medical Director – Professional Standards), Tracy Kean (Deputy Chief Nurse) and Myles Timson (Head of Employee Relations). In accordance with the established terms of the reference, [NUHT0000148] the Group was tasked with ascertaining who accessed the data, when, and for what purposes.

The Investigation Process

173 The process adopted was undertaken in two stages. Stage 1 of the process involved identification of each recorded instance of access to the medical record of each deceased victim concerned utilising the audit trail functionality of the Trust's systems. The manager of each individual who was identified as having accessed a relevant record was then required to undertake a fact-finding meeting with the individual utilising a six-page template [NUHT0000144]. In this meeting the individual was asked about their understanding of the Trust's information governance requirements; their reason for accessing the records; involvement of any other staff; what (if anything) they did with the information they accessed; and, whether they have previously been spoken to or investigated in relation to access to patient records without a legitimate reason. The manager recorded the answers along with their own assessment of the position including legitimacy of access. Access may have been considered legitimate, for example, where it was necessary for direct care purposes, care planning, or carrying out administrative tasks relating to the provision of care.

174 The templates completed by managers following these meetings referred to the Group which met twice a week for review and scrutiny. This included conducting checks against lists of individuals involved in the care provided, shift patterns, and considering the nature and scope of an individual's role. In cases where the Group was not satisfied with responses provided or did not fully understand the reasoning of the manager in the template then further detail was

sought. Where an account was verified and access accepted as being legitimate then the individual was allocated to a "no further action" group. Otherwise, they proceeded to Stage 2 of the process. The Group did not in respect of any case automatically accept the assessment of the manager, and in cases where the Group was not satisfied with the conclusion of the manager then the individual was advanced to Stage 2 of the process.

175 Stage 2 of the process involved a formal investigative process by a third-party human resources consultant, involving a further, detailed scrutiny of access and justification provided for that access by the staff member concerned. All individuals proceeding to Stage 2 were formally notified of the process and provided with terms of reference setting out the investigative framework, procedural roadmap, and expectations. They were also provided with information about their procedural rights, including access to representation, and support mechanisms including wellbeing support [NUHT0000137].

176 The Stage 1 process began on 20 February 2025 and has continued to date. Regular updates were provided to the Incident Command Group with regard to the number of individuals proceeding through to Stage 2.

177 Initial numbers of individuals that accessed the records of the deceased victims were understood to be around 70 in total, with all but 9 of those being staff employed directly by the Trust. Steps were taken to seek to identify who those non-substantively employed staff were. The numbers increased during the period within which the investigations took place. The most recent Stage 1 status report was produced on 10 July 2025 [NUHT0000139] (version 13 of these status update reports). This report sets out that the total number of individuals that had accessed the records of the deceased victims was 98, with 47 of those individuals proceeding to Stage 2 of the process, and 50 having been deemed to be legitimate access. Earlier versions of this document reflected that a number of cases were initially deferred for reasons of ill health, long term absence, or no longer having been employed by the Trust (where contact had been attempted but not yet successfully). The Trust has during this

period sought to contact each of these individuals in order to enable the Stage 1 process to be completed.

Notification to the bereaved families, and third-party bodies

178 Conscious of its duty of candour the Trust gave early consideration to the issue of notification to the families of the deceased. As part of this, contact was also made with colleagues at NHS England on 14 February 2025 [NUHT0000093], and the Trust has remained in contact with them throughout. I subsequently discussed with Dr Sue Elcock the most appropriate way to approach this in the interests of the families, taking into account the earlier contact with Nottinghamshire Healthcare NHS Foundation Trust. It was agreed that the families would be informed as soon as possible, and an offer of a meeting would be made.

179 In accordance with its duty of candour obligations, the Trust wrote to the families of each of the deceased victims to inform them of the potential unauthorised access to the medical records and offering a meeting. Careful consideration was given to the sequence of reporting to the family and other stakeholders with a preference to inform the family in advance wherever possible. On the morning of 19 February 2025 however the Trust was informed by way of an anonymous email that the sender was aware of unauthorised access to records and that the Daily Mail were now also aware [NUHT0000094]. In this context it became imperative to inform the families as soon as possible so that they did not hear of this issue for the first time by way of media reports.

180 Steps were taken the same day seeking the views of NHS England prior to the letter being sent, and our legal representatives Browne Jacobson LLP made contact with the legal representatives of the families to discuss the most appropriate way in which to contact the family. They confirmed that correspondence should be directed to them for onward sharing with the families. Arrangements were made for the solicitor to meet with the families,

and for the duty of candour letters to be provided in advance of then, followed by a call between the families' solicitor and Browne Jacobson LLP. The duty of candour letters was sent on 20 February 2025 [NUHT0000102, NUHT0000100, NUHT0000101].

181 During this time, efforts were made for the Trust Chief Executive, Anthony May, to make contact with the Chief Constable of Nottinghamshire Police to inform them of the matter. Gilbert George also made contact with the Deputy Chief Constable on 20 February 2025. It was agreed that the police would be informed of the outcome of the Trust's internal investigation in due course [NUHT0000096].

182 Following the provision of duty of candour letters and having opened a dialogue via the solicitors for the families, initial queries were raised as to the numbers of individuals involved in accessing the records, when the first stage of the investigation would be complete, and the nature of the records held. At this time, it was understood that around 90 staff were in scope as having potentially accessed records without a legitimate purpose, but that stage 1 of the investigation process would further inform the position.

183 Specifically on the issue of the nature of records that were accessed, the Caldicott Guardian had considered the issue of whether any photos or videos were contained in the records and confirmed that neither were contained in the records, other than a photograph of a bruise on the leg of one victim. In addition, it was confirmed that the Trust does not have the ability to store videos within its records management systems.

184 The families indicated through their representatives that they did not want a meeting with the Trust but requested that they be provided with regular updates with the progress of the Trust's investigation.

185 The Trust recognised the potential seriousness of this matter and therefore formally reported to the General Medical Council [NUHT0000097] on 20

February 2025, and the Nottingham and Nottinghamshire Integrated Care Board was notified on 21 February 2025 [NUHT0000098].

186 On the same day the Trust received a response from the Information Commissioner's Office informing that they had decided that no further action was necessary on the part of the ICO in relation to the notified breach [NUHT0000095]. This was due to the UK GDPR applying only to identifiable living individuals, and as the individuals in concern were deceased at the point of records being accessed then the matter would fall outside of the remit of the Information Commissioner. This response indicated that the Trust should consider a referral to the police and continue its investigation to determine any learning and measures that could be introduced to seek to reduce the likelihood of recurrence of an incident of this nature. A number of recommendations were made.

187 The Trust remained in contact with the Information Commissioner's Office, and on 6 March 2025 [NUHT0000104] emailed to update as to reporting in the national media, the high profile nature of the issue, and that the Trust was in the process of managing the breach including having completed the first stage of an investigation which identified around 24 members of staff who were being taken forward for a second stage investigation/disciplinary panel process. Within this correspondence the Trust indicated that it was considering what steps could be taken with regard to reducing the risk of recurrence, one of which actions included considering the extent of access to systems by front of house reception staff at the main entrance to QMC. This action has since been undertaken and access amended so that no clinical information can be viewed by these members of staff.

188 The matter was also brought to the attention of the Trust Audit Committee. I provided a verbal briefing to the Audit Committee in a confidential meeting on 6 March 2025 [NUHT0000103], and the Audit Committee Chair subsequently produced a report to the Trust Board on this issue [NUHT0000146]. A report

was further presented to a confidential meeting of the Board on 13 March 2025 [NUHT0000138 and NUHT0000106].

Liaison with the bereaved families and appointment of an independent investigator

189 Substantive liaison with the families began via their legal representatives on 21 February 2025 when a number of questions were asked to better understand the nature of the potential unauthorised access and when the issue came to the attention of the Trust. Liaison continued with the families' solicitor as the Trust responded to queries raised [NUHT0000105].

190 On 4 March 2025 Deborah Gladden-Porter reported to the Incident Command Group summarising the findings of the two-stage investigation process to that point in time. The report indicated that it was intended that Christine Woolley would be appointed as external investigator in relation to Stage 2 of the process. It was however noted by the meeting that Christine's appointment may not be deemed as appropriately independent given her previous role as Head of Human Resources for the Trust. Recommendations were made for an alternative appointment.

191 A formal update was provided as to the outcome of Stage 1 on 7 March 2025 [NUHT0000126 and NUHT0000125], advising as to the total number of individuals that had accessed records, and the number being taken forward to Stage 2 of the process. There were various individuals at this time in relation to whom the Stage 1 process was yet to be completed due to long term absence, being off-duty, agency workers, or no longer employed by the Trust. An outline of the Stage 2 process was provided, with the intention for this to commence during week commencing 17 March 2025.

192 Following the concerns raised in the Incident Command Group meeting on 5 March, the Trust explored options for appointment of an external investigator. It was decided to appoint Capsticks LLP HR Advisory Service to provide independent investigatory support to ensure procedural integrity and

impartiality in this Stage 2 process. The external investigator was tasked with systematically collating and evaluating evidence, conducting structured interviews with relevant personnel, and formulating findings in accordance with Trust policy. Terms of Reference for the investigation of medical staff and Agenda for Change staff are exhibited with this statement [NUHT0000149 and NUHT0000150].

193 In order to ensure the robustness of the Stage 1 process, it was also proposed at this time that a "dip-testing panel" be appointed to select a random sample of the cases allocated to the "no further action" group in order to test the robustness of the process and decision making at Stage 1. It was further proposed that the Stage 2 independent investigator would also conduct a similar "dip-testing" exercise.

194 On 17 March 2025 an update was provided to the families' solicitor advising that Stage 1 was considered to be sufficiently progressed as to enable Stage 2 to be commenced [NUHT0000128]. This informed as to the appointment of the external investigator and the terms of reference in respect of Stage 2, seeking any comments or questions from the families on these. It was advised that the investigator would also conduct a random sampling exercise to validate the rationale for decisions in respect of cases where access was deemed to be legitimate.

195 In the same letter the families were advised of safeguards that had been put in place around access to clinical records, as follows:

a) Conducting regular audits every two weeks to check if there was further access to records

b) That all staff had been written to reminding them of responsibilities regarding accessing of records

c) That whilst the Trust core patient electronic records systems do not currently enable the restriction of record access, the Trust had asked

whether the supplier of the system to be used going forwards would look to build this into their future roadmap

196 The families raised comments/questions in relation to the Stage 2 terms of reference on 19 March 2025 [WITN0226003 and NUHT0000107], as well as requesting that the approach in respect of every individual deemed "no further action" in Stage 1 could be audited and the families could meet with the auditor. The Trust considered these requests and declined a meeting with the investigator due to the fact-based nature of the investigation. With regard to the first request, the Trust initially declined to audit all cases on the basis of the low threshold adopted for progression to Stage 2 and rigour applied at Stage 1 of the process.

197 The Trust provided a further update on the position with the investigation on 28 March 2025 [NUHT0000132, NUHT0000131 and NUHT0000134]. Within this the Trust communicated its changed stance with regard to the review of Stage 1, having determined the appointment of a barrister, Robin Hopkins, to complete a review of the determination of each case in the "no further action" group. The Terms of Reference were shared with the families for comments in advance of his review. Comments were provided by the family and the draft Terms of Reference [NUHT0000140] containing those comments were provided to counsel to consider when conducting their review, as well as final Terms of Reference [NUHT0000141] which took those comments into account. Correspondence was received from the parents of Barnaby Webber expressing their dissatisfaction with the action taken by the Trust to this point and requesting that all individuals identified in Stage 1 be taken forward for formal disciplinary processes. Having considered the appropriateness of taking all staff to the Stage 2 process where it had been determined that their access to records had been legitimate, the Incident Command Group determined that an appropriate and proportionate approach would be to appoint an external barrister to review the Stage 1 process and decisions taken in allocating each

case to the "no further action" group. I communicated this decision directly to the parents of Barnaby Webber [NUHT0000142].

198 This letter also informed the bereaved families of the expansion of the Trust's investigation to the surviving victims of the Incident.

Further unauthorised access to records identified

199 Whilst the investigation by the Trust initially focussed on potential inappropriate access to records of the deceased victims due to the context in which the concerns were initially raised with the Trust, the scope of investigation was subsequently broadened to the three surviving victims of the Incident. This followed receipt of correspondence from solicitors representing Mr Wayne Birkett and Miss Sharon Miller dated 20 March 2025 who contacted the Trust seeking information regarding unauthorised access to their clients' records [NUHT0000113]. The Caldicott Guardian obtained and reviewed audit records from the Careflow system used in the Trust Emergency Department as an initial screening exercise, which revealed access that was more likely than not, inappropriate. The judgement of the Caldicott Guardian was reached by taking into consideration the job role of the member of staff concerned timing of access and the location that records were accessed from.

200 The Caldicott Guardian also referred the matter to the Information Commissioner's Office, who responded on 21 March 2025. This referral was given incident number 41678 [NUHT0000111]. The Information Commissioner's Office provided an initial response on 8 April 2025 acknowledging that both referrals related to the incident on 13 June 2023 and asking for an informal call to discuss the matter and progress being made. The Caldicott Guardian responded on the same day by email [NUHT0000122], having not been able to make contact via telephone, providing an update as to the progression of the matter and an indication of the findings to date as well as the decision to appoint an independent barrister to review the process to

date and third party body to conduct the second stage of the disciplinary process investigations.

201 The Trust Data Protection Office again informed the Chief Executive, Anthony May, of the incident on 21 March 2025 in his capacity as Accountable Officer [NUHT0000109].

202 A third surviving victim was identified through media reports but had not contacted the Trust. For the Trust's own due diligence purposes, a review of that individual's audit records was undertaken. The investigation revealed potentially inappropriate access to the records of this individual also.

203 The duty of candour process was initiated for the additional cases, with letters being sent to the solicitor [NUHT0000114] for Mr Birkett [NUHT0000119] and Miss Miller [NUHT0000118], and to Mr Gawronski, on 28 March 2025 [NUHT0000117] confirming the widening of the scope of investigation, the status of the ongoing investigation and arrangements for regular updates in relation to those investigations in relation to those injured people. Mr Gawronski was contacted by the Trust Caldicott Guardian by telephone on 29 March 2025 [NUHT0000124]. The apparent inappropriate access to his records was explained and the Trust apologised. The Caldicott Guardian explained that an investigation was underway, and further action would be managed through the disciplinary process for the staff concerned.

204 The matter was also reported to the GMC [NUHT0000120 and NUHT0000112], and the Trust remained in contact with NHS England and the Nottingham and Nottinghamshire Integrated Care Board throughout this period.

205 Following the identification of potential unauthorised access to the records of the surviving victims the Trust separated its investigation into what have been referred to as Cohort 1 and Cohort 2. Cohort 1 includes those staff that were found to have accessed the records of the deceased victims from 13 June 2023 onwards. Cohort 2 includes those staff that were found to have accessed the records of the living victims from 13 June 2023 onwards. The records for the

latter cohort are larger since the surviving victims were patients of the Trust for an extended period and accordingly received care from a larger number of staff.

206 The Caldicott Guardian agreed to review audit records from the Trust's systems to identify the extent of access and the extent to which such access was considered to be legitimate. This was an ongoing process complicated by the fact that there was a significant number of accesses to the records, and that these individuals continued to receive ongoing care from the Trust. The exercise undertaken by the Caldicott Guardian revealed 260 individuals as "in scope" for review, and of these to date 169 have been determined as legitimate access via the Stage 1 process, 35 are progressing to a Stage 2 process. A cross-referencing exercise was undertaken to identify any individuals who were identified as accessing the records of the surviving victims yet progressed to Stage 1 in respect of access to the records of deceased victims. 22 individuals were identified and their access to the surviving victims' records has been considered as part of the Stage 2 process in respect of the deceased victims.

207 On 9 April 2025 a confidential briefing was provided by email to the Trust Board explaining the issue and the actions taken to that point [NUHT0000123].

Ongoing liaison with the bereaved families and surviving victims

208 Since the end of March 2025, the Trust has remained in constant dialogue with the bereaved families and two of the surviving victims. The third surviving victim, Mr Gawronski, indicated in conversation with the Caldicott Guardian that he would contact the Trust if he had any queries but otherwise, he was content for the outcome of the investigation to be provided to him on conclusion. Regular updates have been provided on either a weekly or fortnightly basis to the solicitors respectively representing the bereaved families or surviving victims.

209 These updates informed the bereaved families and the surviving victims of the processes being undertaken, the progress in relation to those processes, ongoing actions, and responding to any ad hoc queries raised. Updates were

provided to the solicitor acting for the bereaved families on: 3, 11 and 25 April; 2, 20 and 30 May; 9 and 13 June; 1 July and 14 July 2025 [NUHT0000172, NUHT0000174, NUHT0000175, NUHT0000178, NUHT0000179, NUHT0000180, NUHT0000182, NUHT0000183, NUHT0000185, NUHT0000187]. Similarly, updates have been provided to two of the surviving victims' solicitors on 2 and 11 April; 2 and 30 May; 13 June; 1 July 2025, 14 and 15 July 2025 [NUHT0000171, NUHT0000173, NUHT0000177, NUHT0000181, NUHT0000184, NUHT0000186, NUHT0000188, NUHT0000189].

Potential additional identification of access to records

210 During the course of the above process a concern has been raised as to the extent of audit data that has been reviewed from across the Trust's core patient systems and whether all such relevant data has been captured and taken into account. The Trust is in the process of reviewing the position in this regard, and where it is identified that there are additional individuals that may have accessed records of either the deceased or surviving victims potentially without a legitimate purpose then the same two stage investigative process will be undertaken as explained above, and the Trust will keep the bereaved families and surviving victims informed of progress as part of its ongoing dialogue with them.

LOOKING FORWARD

211 As is clear from the chronology above, the Trust's investigation of this matter is ongoing. At the time of providing this statement to the Inquiry the Stage 2 process is largely complete in respect of Cohort 1 (subject to five final investigation reports being produced in relation to individual members of staff and which are outstanding) but has yet to commence in relation to Cohort 2. The Stage 1 process in respect of Cohort 2 is progressing.

212 When each Stage 2 investigation process is completed by the external investigator then the next step is for the outcome of that investigation in respect of each individual staff member concerned to be considered by an appointed

case manager (Deputy Medical Director or Deputy Chief Nurse) to determine the next steps to be taken in relation to each individual.

213 The outcome of the investigation will result in one of the following. As a low threshold approach was adopted to progressing cases to Stage 2 of the process to ensure a robust investigation of this matter, further detailed investigation may reveal that there are cases where access was legitimate and no further action is required. Those cases will not proceed further. Alternatively, where the Stage 2 investigation has revealed concerns with regard to unauthorised access then the staff member will proceed to a disciplinary panel, and a formal employment process will be followed. The action to be taken will be determined by that disciplinary panel. In the case of regulated professionals, consideration will be given to the appropriateness of making a referral to their relevant professional regulatory body. In all cases the Trust will make referrals to the police where this is considered appropriate.

Communications to staff since identification of the concerns

214 Whilst the investigation into potential unauthorised access to records has been ongoing, the Trust has taken the opportunity to communicate on a number of occasions to staff in relation to the issue of unauthorised access to patient records with a view to highlighting this issue and seeking to mitigate against further unauthorised access.

215 A message was sent to all staff on 24 February 2025 focussed solely on the issue of unauthorised access to records. This was headed "Reminder of Professional Responsibility – Appropriate Access to Records". It reminded staff of the importance of patient confidentiality and the potential consequences of unauthorised or inappropriate access to patient records. Staff were also referred to the Caldicott Guardian in the event that they had any queries or required additional guidance [NUHT0000205].

216 On 27 February 2025 a reminder was sent to all staff of the Trust through a "Trust Briefing", a regular staff update sent by email [NUHT0000207]. An

internal communication was sent by email on 4 March 2025 headed "Appropriate access to records" reminding staff of their obligations [NUHT0000193]. This was published on the Trust intranet the same day. Further communication was sent to all staff on 6 March 2025 informing them of the publication of an article in the Mirror relating to this matter, and the ongoing investigation by the Trust as well as reminding staff of their professional and legal responsibilities regarding the appropriate access to and use of patient records [NUHT0000199].

217 On 20 March 2025 the Trust provided a video in "Trust Briefing" to all staff, which was also made available on the Trust intranet, in which the Trust Chief Executive addressed the issue of access to records stating: *"I want to say something about access to records. A couple of weeks ago, you all received an e-mail from our medical director, chief nurse and chief people officer. I want you to make sure you read that e-mail. It's extremely important that you use and share data and records appropriately. If you don't, the consequences can be serious for you and they can be serious for our patients and their families. So please read the e-mail you were sent on the 4th of March and take heed of what it says".*

218 Following the outcome of the ongoing investigatory and disciplinary processes the Trust intends to carefully consider the communication of the outcome of these cases, including highlighting any disciplinary action taken in relation to any member of staff involved so as to give a clear understanding of the actions that may follow the unauthorised access to medical records in a real life and local context. The Trust will carefully consider its communications highlighting the potential consequences of such matters, whilst seeking to avoid unnecessary scaremongering, or creating concerns from staff where access to records is appropriate and legitimate. The Trust is conscious of the need to strike the right balance here in the interests of service users.

Information Governance Review

219 As part of its work the Incident Command Group raised concerns as to the lack of escalation or appreciation of the high-profile nature of the Incident to which the unauthorised access to records in this matter relates. A decision was made to investigate this issue. The investigation report produced by the Data Protection Officer [NUHT0000161] made several recommendations, including a definition of a "high-profile" case with a view to steps being inserted into relevant patient safety, data protection and human resources policies to consider whether a case should be deemed to be high-profile.

220 The progress of recommendations made is tracked through the Data Protection and Cyber Security Panel and a Data Breach Action Tracking log has been retained, the most up to date version of which at the time of this statement being produced was May 2025 [NUHT0000197].

221 A definition has been approved for a "high-profile" breach as "an incident that attracts significant attention or publicity, potentially damaging the reputation of the Trust". This definition has been incorporated into the Trust's Data Breach Process [NUHT0000156] providing that "this is to ensure all parties as part of the process internally processing data breaches are mindful for this and can escalate at the earliest opportunity to senior management via the incident handler".

Identification of trends and consideration of further action

222 It is expected that the above exercise in relation to both Cohort 1 and Cohort 2 will identify any potential trends or themes in relation to non-compliance with the Trust's polices with regard to illegitimate access to patient records. The issues that the external investigator has been asked to consider with each individual addresses: the justification for access, factors influencing access, compliance with security measures, and prior conduct and training. Whilst the outcome of the consideration of each individual case will inform the action to be taken in that case, the Trust acknowledges that wider analysis of the

investigation's outcomes may provide a deeper insight from which the Trust can learn lessons from , and which may inform changes on a wider level.

223 The Trust is committed to gaining any learning it can in relation to this matter and intends to conduct a deeper analysis of the data following completion of the Stage 2 process in respect of both Cohort 1 and Cohort 2.

224 With regard to Cohort 1, the majority of the reports from the external investigator were issued in late June 2025 together with an overarching summary report, both in relation to Agenda for Change staff [NUHT0000200] and medical staff [NUHT0000151]. At the time of providing this statement the Trust has not considered these recommendations in detail or actioned these but will consider them through appropriate governance routes with a view to determining what if any action to take going forwards.

Systems developments

225 The Trust is currently in the process of replacing its patient administration system ('PAS'), Careflow, with a new system, Nervecentre. Whilst Nervecentre is currently used by the Trust for certain functionality, as described above, it will from October 2025 be taking over the wider PAS functions that are currently handled by the Careflow system. The Careflow system was implemented around 13 years ago and the Trust's current contract in respect of that system will end in November 2025. The Trust has been working closely with Nervecentre to replace the PAS elements conducted within Careflow with the system provided by Nervecentre. Upon implementation of the additional Nervecentre functionality, the Careflow system will be decommissioned.

226 During this investigation the Incident Command Group has considered the capability of the various different elements of the Trust's systems including the following:

a) Locking Down Records – consideration has been given to whether it is possible within the Trust's existing systems to lock down records in

respect of specific individuals, namely the victims of the Incident. The Incident Command Group allocated an action for the Caldicott Guardian and Senior Information Risk Owner to explore the possibility of such functionality being built into the Nervecentre system that is to replace Careflow.

Initially they contacted Nottinghamshire Healthcare NHS Foundation Trust to understand the system they use [NUHT0000204 and NUHT0000192], the approach that they adopt, and to inform the approach to Nervecentre. It was established that Nottinghamshire Healthcare NHS Foundation Trust utilise a system known as "RiO" and that within that system there is the potential for records to be locked down and/or access "challenges" displayed when a member of staff attempts to access a record.

In this knowledge, Andy Callow sought to understand whether something similar was achievable within the Trust's systems. The outcome of this is that it is understood that the current Careflow system has basic functionality to apply sensitivity to a patient record, which enables the patient's address, GP practice and contact details to be hidden. This however does not interface with many of the Trust's downstream systems, which means that such hidden information cannot be processed by those systems. This raises significant concerns as to clinical safety. For this reason, this feature has not been utilised by the Trust to date. It is also possible to tag a record with a "Do Not Disclose Information" alert, and which does interface with downstream system. However, this does not restrict access to a record but instead presents an alert to the individual seeking to access the record. As the Trust is soon to replace the Careflow system, further steps have not been taken with regard to developing any additional features within Careflow and the focus has been to seek to work with Nervecentre to explore the development of the functionality of that system.

Nervecentre has no in-built functionality to restrict access to a record. Andy Callow and Jeremy Lewis are working with Nervecentre to determine what can be achieved by way of additional functionality and have raised a "feature request" in this regard [NUHT0000203].

b) Break Glass – in considering the current functionality of its systems the Trust has also raised the question of whether some form of "break glass" functionality would be appropriate to use, whether in relation to high profile cases only or more generally. This would involve individuals being challenged when accessing a record as to the reason for them doing so and potentially requiring an active step to be taken to either select one of a number of options from a drop-down list before being granted access, or actively clicking a button to confirm access is legitimate.

   Again, this functionality is not currently built into the Nervecentre system. The possibility of such feature being developed within the Nervecentre system is being explored further as part of the conversations to take place between Nervecentre, Andy Callow and Jeremy Lewis.

227 Whilst the Trust intends to explore these potential system options, it is aware they are utilised to some extent by other trusts locally and nationally. Careful consideration is therefore required before implementing any such options. It is necessary to consider the potential options both from a systems capability perspective (including the interface with downstream systems and "knock-on" effects of features of the overall patient administration system), but also from a substantive and clinical safety perspective. Any future developments must be considered in the context of the practicalities of the need to provide efficient access to records to support safe provision of emergency, urgent and scheduled care to patients. This involves large numbers of staff in many aspects of care. The identity and role of those needing access to records for specific patients cannot be reliably and completely identified in advance of that access being necessary, even for planned care purposes. These issues are

explicitly recognised in the national policy position referred to above, including the outcome of the Caldicott Information Governance Review and work of the NDG referred to above.

228 These are complex and involved considerations that require the input of various individuals including the Caldicott Guardian, Data Protection Officer, and Senior Information Responsible Officer. The Trust is concerned to ensure that it does not adopt a "knee jerk" reaction to specific incidents but adopts a measured and informed approach that ensures a clinically safe method in an environment where care and treatment is delivered to patients across a range of disciplines and to which access to patient level information is required for the safe and effective delivery of care.

229 At the time of submitting this statement the Trust is continuing to work with Nervecentre to fully understand the options available to it, and what the functionality of those options might look like and can achieve. Having done so the Trust will then undertake further detailed consideration of what that functionality might mean in practice, the impact it is likely to have upon unauthorised access to records, and any potential impacts upon the safe and effective delivery of care and treatment before taking any decision to proceed with any potentially available option.

Changes to role-based access during the course of this investigation

230 As part of Stage 1 of the investigation process the appointed Task and Finish Group reviewed the responses provided in the template forms completed by managers of staff who had accessed the records of the victims. In doing so they identified a concern relating to systems access of reception staff at the main entrance of QMC. It was identified that these reception staff had been afforded the same level of access to systems as receptionists working on wards. This gave them access to a level of information relating to patients that, whilst appropriate for receptionists on a ward, is not required for their role as reception staff at the main entrance to the hospital. Steps have been taken to

amend this position so that these reception staff now have access only to non-clinical information in a patient's record.

Processes and procedures

231 In addition to the issue of potential additional functionality within its systems, including those to be implemented shortly, the Trust has considered what additional processes and procedures it can put in place to assist in the identification of potentially unauthorised access to records.

232 Consideration is being given as to the measures that could be introduced generally and/or specifically in relation to high-profile cases.

233 I refer below to ongoing dialogue with the Trust's internal auditors, 360 Assurance, which has identified that several trusts do conduct some form or audit or review process in respect of the legitimacy of access to records on a regular basis. The Trust Senior Information Risk Owner is seeking further information as to how this works in practice, including how many records are checked and how decisions are made as to which records are to be checked.

234 Further information is being sought as to size and nature of the trusts who conduct proactive audit or review exercises. A key issue for the Trust in this regard is its size, with around 350 million database rows added and 150 million database updates every day. Whilst it is recognised that such proactive exercises may be effective in smaller trusts, there are questions over the extent to which this would prove to be an effective mechanism within the Trust.

235 Consideration is also being given to the potential for some form of automated route in the longer term, with a view to exploring the options available. Such considerations are at a very high-level initial stage as the Trust considers all potential improvements to its current processes. This again requires further detailed consideration as to the possibility and effectiveness of any such process. The initial concern of the Trust in seeking to utilise such an approach is the lack of clinical expertise that would be involved, and that is a necessary

prerequisite to the audit process. It is necessary, particularly in an organisation the size of the Trust and which handles such a broad range of disciplines, for clinical expertise to be applied in order to match the condition of a patient to a role and assess whether accesses to a record are consistent with an episode of care. Without this clinical element it is difficult to envisage how an audit or review process might be effective.

Identifying and addressing wider concerns

236 The unauthorised access to patient records in relation to the Incident is not the first experience of the Trust in this regard. During 2022 the Trust ran a communications campaign [NUHT0000194] aimed at raising awareness of data issues, and which included the use of various posters that had been used by another NHS trust previously [NUHT0000201 and NUHT0000198].

237 Concerns have since that time been raised by the Trust Data Protection Officer in bi-annual briefings for the Audit Committee dated 15 June 2023 [NUHT0000152], 7 January 2024 [NUHT0000157], 6 June 2024 [NUHT0000158], 2 January 2025 [NUHT0000159] and 19 June 2025 [NUHT0000170]. These briefings raise concerns as to data breaches occurring within the Trust and the extent of these that concern unauthorised access to medical records and requiring reporting to the Information Commissioner's Office, as well as concerns as to mandatory training compliance rates.

238 Throughout 2025 the Data Protection Officer has also provided bi-monthly rolling summaries of data breaches to the Audit Committee, each one of which has noted concerns as to unauthorised access to medical record [NUHT0000160, NUHT0000167 and NUHT0000169].

239 The Trust is conscious that the issues identified with regard to potential unauthorised access to medical records could indicate wider concerns over culture, and whilst many of these cases involve a single individual accessing a single record this is not always the case and the Trust understands the importance of it being clear with regard to appropriate access to records of

service users. In all cases identified in the bi-annual briefings of the Data Protection Officer the Trust had carried out an investigation to establish whether there has been unauthorised access to records, with each case considered on its own merits in terms of the action taken.

240 In addition to the campaign that was run in 2022, during the period from 2024 there have been various actions ongoing from a data protection perspective within the Trust and with a view to ensuring compliance with the obligations of the Trust in this area. This has included:

a) Branding of the information governance function to ensure coherence with the overall strategy and culture of the Trust

b) Establishment of a new intranet website to promote the provision of the right information in an accessible way [NUHT0000195 and NUHT0000051]

c) Developing a new Data Protection and Security Handbook in both digital and hard copy format [NUHT0000196]

d) A detailed review of information governance policies

241 A recommendation from Audit Committee in light of concerns that have been raised has been for a meeting to take place between Marc Wilson (Data Protection Officer), Paul Matthew (Chief Financial Officer), Danielle Petch (Chief People Officer), Myles Timson (Head of Employee Relations), and Andy Callow (Senior Information Risk Owner) with a view to discussing and producing a joint human resources and information governance action plan. That meeting took place on 30 October 2024 and resulted in a number of actions that have been tracked subsequently [NUHT0000162]. These actions include the employment pack for new starters including a welcome from the Data Protection Office [NUHT0000008], an ongoing review of mandatory data protection training [NUHT0000009], the review of existing confidentiality clauses in employment contracts, development of an incident scoring matrix to

be used in human resources matters involving unauthorised access to records [NUHT0000168], and a communications campaign around matters of data protection and confidentiality.

242 The Trust has, via its Data Protection Office developed a data breach campaign with communications colleagues. The campaign commenced on 10 July 2025 [NUHT0000206] and will run until May 2026. The campaign, *"Your Responsibility, Your Actions, Their Privacy"* is directed at staff at all levels and is intended to assist in promoting a positive culture around data protection and security, including with regard to appropriate access to patient records. A communications plan has been developed and is exhibited to this statement [NUHT0000190], together with draft posters to be utilised as part of the campaign [NUHT0000191]. The campaign will be evaluated at its end date to determine the success and/or effectiveness of it.

Understanding the approach adopted by others

243 To inform its considerations the Trust has asked its internal auditor, 360 Assurance, to conduct a benchmarking exercise against the approaches of other NHS trusts with regard to seeking to prevent unauthorised access to records [NUHT0000202]. A process is currently ongoing with regard to a survey which has been circulated to other NHS trusts that are audited by 360 Assurance to develop an understanding of the approach taken by others. At the time of submitting this statement, returns were relatively low, but in respect of those who had responded the following has been identified:

a) Other NHS trusts take proactive measures which the Trust may consider implementing with regard to mitigating against unauthorised access to records.

b) Two NHS trusts have confirmed they conduct proactive audits/review, in addition to reactive investigations and handling of breaches – further exploration of the extent of what these NHS trusts do is required.

c) One NHS trust uses a system called FairWarning, which is a patient privacy intelligence tool used to detect unauthorised access to patient data across clinical system – the Trust explored this option a number of years ago but it was found to be ineffective due to the extent of results it provided. Notwithstanding this a demonstration of the system as it currently operates is being arranged with the provider company to better understand what this might offer at the current time.

d) All the NHS trusts that responded to date have role-based access controls in place, similarly to the Trust, but also have some form of break glass functionality.

e) There has been a mixed response as to locking down high-profile service user records and no consistent approach is adopted.

f) All organisations have policies and training regarding access to patient records, and which are confirmed as being read and understood by all members of staff – though different mechanisms are used by different NHS trusts; and

g) At present no NHS trust that has responded to date uses artificial intelligence to automate and monitor system access.

244 360 Assurance continue the survey exercise and are expected to provide a detailed summary of responses when there has been a greater return from the NHS trusts surveyed. The Trust intends to take into account the outcome of this survey exercise when considering what further steps it may put in place in relation to the prevention of unauthorised access to patient records.

CONCLUSION

245 By way of this detailed statement the Trust has sought to assist the Inquiry in its understanding and consideration of this matter so far as it concerns the Trust, and the unauthorised access to medical records of the victims of the

Incident. The Trust is committed to learning from this experience as well as ensuring that appropriate action is taken in relation to those individuals who are found to have accessed these records without a legitimate reason for doing so.

1. The Trust will assist the Inquiry with any further questions or enquiries following its consideration of this statement.

Statement of Truth

I believe the content of this statement to be true. I understand that proceedings may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief of its truth.

Signature

GRO-B

Dr MANJEET SHEHMAR, MD, FRCOG, MBBS, BSc

Dated: _5th December 2025

Index to First Witness Statement of Nottingham University Hospitals NHS Trust

Exhibit No.	Document Description	Inquiry URN
1	The Nottingham University Hospitals National Health Service Trust (Establishment) and the Nottingham City Hospital National Health Service Trust and the Queen's Medical Centre, Nottingham, University Hospital National Health Service Trust (Dissolution) Order 2006	NUHT0000069
2	Department of Health and Social Care Confidentiality Code of Practice	NUHT0000016
3	Guidance to the Department of Health and Social Care Confidentiality Code of Practice	NUHT0000028
4	Information Security Management Code of Practice	NUHT0000049
5	The Health and Social Care Information Centre Guide to Confidentiality 2013 (updated March 2022)	WITN0226004
6	General Medical Council's guidance document 'Confidentiality: Good Practice in Handling Patient Information	NUHT0000044
7	General Medical Practice Code of practice "Good Medical Practice"	NUHT0000045
8	National Midwifery Council Code of Practice	NUHT0000058
9	HCPC 'Guidance on Confidentiality'	NUHT0000017
10	Caldicott Committee's Report on the Review of Patient-NUHT0000029 Identifiable Information	NUHT0000029
11	NHS Contract Particulars and Service Conditions	NUHT0000002
12	Caldicott Information Governance Review	NUHT0000010
13	National Data Guardian 2023/24 Annual Report	NUHT0000054
14	National Data Guardian 2020 Survey Report	NUHT0000055
15	Review of Data Security, Consent and Opt-Outs Toolkit	NUHT0000027

16	Report of the Mid Staffordshire NHS Foundation Trust Public Inquiry Volume 1 Analysis of evidence and lessons learned	NUHT0000003
17	CQC Guidance on Background to the duty of candour	NUHT0000013
18	CQC Key Lines of Enquiry	NUHT0000004
19	Information Governance Management Framework	NUHT0000034
20	Data Protection, Confidentiality and Disclosure Policy	NUHT0000026
21	Conduct, Behaviour and Disciplinary Policy and Procedure	NUHT0000060
22	Conduct, Capability and Ill Health Procedure for Medical Practitioners (HR/P&C/016)	NUHT0000015
23	Information Security and Risk Policy (GG/INF/002)	NUHT0000031
24	Information Governance Management Framework (GG/INF/035b)	NUHT0000050
25	Information Governance Policy (GC/INF/035a)	NUHT0000043
26	Data Protection Policy (GG/INF/034)	NUHT0000042
27	Confidentiality Policy (GG/INF/033)	NUHT0000041
28	Health Records Management Policy (GG/INF/006)	NUHT0000032
29	Corporate Records Management Policy	NUHT0000033
30	Social Media Policy (GG/CM/053)	NUHT0000030
31	Records Management: NHS Code of Practice	NUHT0000057
32	Mandatory Training Policy	NUHT0000047
33	NHS Core Skills Training Framework	NUHT0000025
34	Temporary Staffing Policy	NUHT0000046
35	NHS Digital Data Security Awareness training course	NUHT0000056
36A	NUH Specific Information Governance Training [Video]	WITN0226002A
36B	NUH Specific Information Governance Training [Transcript]	WITN0226002B
37	Data Protection and Security Training	NUHT0000009
38	Information Governance and Data Protection at NUH - April 2022	NUHT0000048

39	Information Governance and Data Protection at NUH - August 2024	NUHT0000008
40	Intranet welcome message from the Data Protection Officer on the Trust	NUHT0000051
41	AfC Apprentice Contract	NUHT0000011
42	AfC General Contract	NUHT0000012
43	Medical Consultant Contract	NUHT0000052
44	Medical Locum Consultant Contract	NUHT0000053
45	Resident Doctor Contract	NUHT0000059
46	Specialist Grade Contract	NUHT0000061
47	Specialty Doctor Contract	NUHT0000062
48	Trust Grade Doctor Contract	NUHT0000068
49	Information Governance and Digital Services Security Incident Management Procedure for Personal Data Breaches	NUHT0000006
50	Data Protection Security Investigation Checklist	NUHT0000007
51	Reporting requirements spreadsheet	NUHT0000063
52	Core systems access matrix	NUHT0000024
53	Datix Audit Request – Systems Audit guidance	NUHT0000014
54	Access permissions of the core patient systems	NUHT0000018
55	Email correspondence RS email to Justine Rosser Notts HC cc Taryn Milton dated 8 October 2024	NUHT0000070
56	Email correspondence from Joy Fisher dated 10 October 2024	NUHT0000071
57	Email correspondence from TM to MW dated 14 October 2024	NUHT0000072
58	Email correspondence from RS email to Joy Fisher cc Taryn Milton dated 14 October 2024	NUHT0000073
59	Email correspondence from Joy Fisher dated 16 October 2024	NUHT0000074

60	Email correspondence from Taryn Milton to Joy Fisher dated 17 October 2024	NUHT0000078
61	Email correspondence from JF Legal dated 17 October 2024	NUHT0000076
62	Email correspondence to Joy Fisher dated 20 October 2024	NUHT0000080
63	Email correspondence from Joy Fisher dated 20 October 2024	NUHT0000079
64	Email correspondence from Joy Fisher dated 9 December 2024	NUHT0000081
65	Email correspondence dated from Joy Fisher dated 24 December 2024	NUHT0000089
66	Email correspondence from HR to CHS dated 20 January 2025	NUHT0000090
67	Data Security and Protection Toolkit ICO referral	NUHT0000092
68	Email correspondence from DPO to CEO dated 13 February 2025	NUHT0000091
69	Bundle of logs of Incident Command Group from 13 February 2025 to 8 July 2025	NUHT0000145
70	Audit trails of access	NUHT0000147
71	Briefing Note on Data Breach by the Caldicott Guardian	NUHT0000136
72	Briefing Note on Data Breach by DPO	NUHT0000135
73	Terms of Reference Task and Finish Group	NUHT0000148
74	Fact finding meeting template	NUHT0000144
75	Confirmation of Investigation information	NUHT0000137
76	Stage 1 status report 10 July 2025	NUHT0000139
77	NHSE briefing re family notification	NUHT0000093
78	Email received from anonymous source about breach	NUHT0000094
79	Duty of Candour Letter Mr Coates	NUHT0000102
80	Duty of Candour Letter Dr Kumar and Dr O'Malley Kumar	NUHT0000100

81	Duty of Candour Letter Mr and Mrs Webber	NUHT0000101
82	Email correspondence, DCC	NUHT0000096
83	Email correspondence NUH to GMC dated 20 February 2025	NUHT0000097
84	Email correspondence from NUH to ICB dated 20 February 2025	NUHT0000098
85	Email correspondence from ICO dated 19 February 2025	NUHT0000095
86	Email correspondence from NUH to the ICO dated 6 March 2025	NUHT0000104
87	Audit Committee minutes 6 March 2025	NUHT0000103
88	Confidential Chairs Report of the Audit Committee	NUHT0000146
89	Data Breach Stage 1 Report - 13 March 2025 Final Report to Board	NUHT0000138
90	Extract of the Board Member Minutes of the Confidential Meeting dated 13 March 2025	NUHT0000106
91	Email from Charlotte Harpin (Browne Jacobson) to Neil Hudgell (Hudgell Solicitors), Lindsay Allison (Hudgell Solicitors) and Manjeet Shehmar (NUHT). re: Nottingham University Hospitals NHS Trust Duty of candour letters - potential data breach	NUHT0000105
92	Weekly update email dated 7 March 2025 from Charlotte Harpin (Browne Jacobson) to Neil Hudgell (Hudgell Solicitors), Lindsay Allison (Hudgell Solicitors), Manjeet Shehmar (NUHT)	NUHT0000126
93	Letter from Charlotte Harpin (Browne Jacobson) dated 7 March 2025 to Neil Hudgell (Hudgell Solicitors), re: Update on Stage 1 Potential Data Breach Investigation	NUHT0000125
94	Terms of Reference - Investigation - Medical Staff	NUHT0000149
95	Terms of Reference - Investigation - Agenda for Change	NUHT0000150

96	Letter dated 17 March 2025 from Charlotte Harpin (Browne Jacobson) to Neil Hudgell [Hudgell Solicitors], re: Update on Potential Data Breach	NUHT0000128
97	Email dated 19 March 2025 - Questions from family	WITN0226003
98	Letter 19 March 2025 from Neil Hudgell (Hudgell Solicitors) to Charlotte Harpin (Browne Jacobson) re: Data Breach Investigation: Draft Terms of Reference	NUHT0000107
99	Email dated 28 March 2025 from Charlotte Harpin (Browne Jacobson LLP) to Neil MH (Hudgell Solicitors) and Lindsay Allison (Hudgell Solicitors) re: Weekly update	NUHT0000132
100	Letter dated 28 March 2025 from Charlotte Harpin (Browne Jacobson) to Neil Hudgell (Hudgell Solicitors) and Lindsay Allison (Hudgell Solicitors) re: Weekly update: week ending 28 March 2025	NUHT0000131
101	[Draft] Terms of Reference Review into Stage 1 Outcomes Legitimate Access Determinations	NUHT0000134
102	Family's comments on Draft Terms of Reference	NUHT0000140
103	Terms of Reference Review into Stage 1 Outcomes Legitimate Access Determinations	NUHT0000141
104	Email dated 25 March 2025 from Manjeet Shehmar (NUHT) to Elizabeth Coleman (NUHT), Gilbert George (NUHT), Andy Callow (NUHT) and others, re: Fw: Data breach investigation	NUHT0000142
105	Email dated 28 March 2025 from Greg Almond (Rother Bray) to Manjeet Shehmar (NUHT), Elizabeth Coleman (NUHT), George Gilbert (NUHT) and others re: Letter to NHS re authorised access to records	NUHT0000113
106	Data Security and Protection Toolkit for Reported Incident Reference 41678 by Jeremy Lewis (NUHT)	NUHT0000111
107	Email dated 8 April 2025 from Jeremy Lewis (NUHT) to SMB-DPO (NUHT)	NUHT0000122

108	Email dated 21 March 2025 from Marc Wilson (NUHT) to Anthony May (NUHT) and Andy Callow (NUHT), re: ICO REPORTED INCIDENT: Data Breach: DB525722	NUHT0000109
109	Email dated 28 March 2025 from Manjeet Shehmar (NUHT) to Rebecca Howard (Rothera Bray), Greg Almond (Rothera Bray), Elizabeth Coleman (NUHT) and others, re: Letter to NHS re unauthorised access to records	NUHT0000114
110	Letter dated 28 March 2025 from Dr Manjeet Shehmar (NUHT) to Mr Wayne Birkett, re: Potential data breach investigation	NUHT0000119
111	Letter dated 28 March 2025 from Dr Manjeet Shehmar (NUHT) to Ms Sharon Miller, re: Potential data breach investigation	NUHT0000118
112	Letter dated 28 March 2025 from Dr Manjeet Shehmar (NUHT) to Mr Gawronski, re: Potential data breach investigation	NUHT0000117
113	Datix logging call to Mr Gawronski of 29 March 2025	NUHT0000124
114	Email dated 28 March 2025 from Manjeet Shehmar (NUHT) to Dmitrije Sirovica (Browne Jacobson) and Emily Hammond (NUHT) re: Further breach briefing	NUHT0000120
115	Email dated from Manjeet Shehmar (NUHT) to Rebecca Howard (Rothera Bray), Greg Almond (Rothera Bray), Elizabeth Coleman (NUHT) and others, re: Letter to NHS re unauthorised access to records	NUHT0000112
116	Email from Jack Adlam (NUHT Communications) to NUHT Staff re: Confidential Board Brief: Data breach update	NUHT0000123
117	Email from Browne Jacobson to Hudgell Solicitors re. update on investigations dated 3 April 2025	NUHT0000172
118	Email from Browne Jacobson to Hudgell Solicitors re. update on investigations dated 11 April 2025	NUHT0000174

119	Email from Browne Jacobson to Hudgell Solicitors re. update on investigations dated 25 April 2025	NUHT0000175
120	Email from Browne Jacobson to Hudgell Solicitors re. update on investigations dated 2 May 2025	NUHT0000178
121	Email from Browne Jacobson to Hudgell Solicitors re. update on investigations dated 20 May 2025	NUHT0000179
122	Email from Browne Jacobson to Hudgell Solicitors re. update on investigations dated 30 May 2025	NUHT0000180
123	Email from Browne Jacobson to Hudgell Solicitors re. update on investigations dated 9 June 2025	NUHT0000182
124	Email from Browne Jacobson to Hudgell Solicitors re. update on investigations dated 13 June 2025	NUHT0000183
125	Email from Browne Jacobson to Hudgell Solicitors re. update on investigations dated 1 July 2025	NUHT0000185
126	Email from Browne Jacobson to Hudgell Solicitors re. update on investigations dated 14 July 2025	NUHT0000187
127	Email from Browne Jacobson to Rothera Bray re. update on investigations dated 2 April 2025	NUHT0000171
128	Email from Browne Jacobson to Rothera Bray re. update on investigations dated 11 April 2025	NUHT0000173
129	Email from Browne Jacobson to Rothera Bray re. update on investigations dated 2 May 2025	NUHT0000177
130	Email from Browne Jacobson to Rothera Bray re. update on investigations dated 30 May 2025	NUHT0000181
131	Email from Browne Jacobson to Rothera Bray re. update on investigations dated 13 June 2025	NUHT0000184
132	Email from Browne Jacobson to Rothera Bray re. update on investigations dated 1 July 2025	NUHT0000186
133	Email from Browne Jacobson to Rothera Bray re. update on investigations dated	NUHT0000188

134	Email from Browne Jacobson to Rothera Bray re. update on investigations dated 15 July 2025	NUHT0000189
135	Article published on NUH Intranet entitled Reminder of Professional Responsibility Appropriate Access to Patient Records, published on 24 February 2025	NUHT0000205
136	Email to NUH Staff re. Trust Briefing - 27 February 2025	NUHT0000207
137	Email dated 4 March 2025 from SMB Internal Comms (NUHT), re: Appropriate access to records	NUHT0000193
138	Email dated 6 March 2025 from SMB Internal Comms (NUHT) to NUH All Users (NUHT), re: National media coverage this evening	NUHT0000199
139	Report compiled by Data Protection Office	NUHT0000161
140	Report dated May 2025, compiled by unknown Re: Data Breach Action Tracking – May 2025	NUHT0000197
141	Policy Document on Data Breach Process	NUHT0000156
142	Capsticks report dated 01/06/2025 regarding alleged Inappropriate Access to Medical Records (agenda for change)	NUHT0000200
143	Capsticks report dated 01/06/2025 regarding alleged Inappropriate Access to Medical Records (Medics)	NUHT0000151
144	Email dated 7 July 2025 from Robin Smith, re: Reminder of Professional Responsibility - appropriate access to patient records	NUHT0000204
145	Email dated 27 February 2025 from Andy Callow (NUHT) to Manjeet Shehmar (NUHT), Tracy Pilcher (NUHT), Anthony May (NUHT) and others, re: Restricting System Access - A Summary	NUHT0000192
146	Email from Paul Volkaerts [Nerve Centre Software] to Andy Callow [NUHT] and Jeremy Lewis [NUHT], re:	NUHT0000203

	Enhancements to safeguards around medical record confidentiality	
147	IG campaign DRAFT Communications Plan	NUHT0000194
148	Patient Confidentiality Poster Campaign	NUHT0000201
149	Patient Confidentiality Poster Campaign	NUHT0000198
150	Minute of Audit Committee Meeting including DPO Briefing dated 15/06/2023	NUHT0000152
151	Minute of Audit Committee Meeting including DPO Briefing dated 7 January 2025	NUHT0000157
152	Audit Committee Meeting, Annual Independent DPO briefing dated 6 June 2023	NUHT0000158
153	Audit Committee Meeting, Annual Independent DPO briefing dated 2 January 2025	NUHT0000159
154	Audit Committee Meeting, Annual Independent DPO briefing dated 19 June 2025	NUHT0000170
155	NUH DPO - Data Breach Report (Rolling Short Summary) January 2025 (as at 24 February 2025)	NUHT0000160
156	NUH DPO - Data Breach Report (Rolling Short Summary) April 2025	NUHT0000167
157	NUH DPO - Data Breach Report (Rolling Short Summary) June 2025	NUHT0000169
158	Intranet published information - What is a data breach/incident. What is a Datix	NUHT0000195
159	Data Protection Employee Handbook	NUHT0000196
160	NUH Data Breaches Human Resources (Audit Committee) Action Plan	NUHT0000162
161	NUH Data Breaches guidance (information governance), Incident Score Matrix for HR purposes	NUHT0000168
162	Trust Briefing 10 July 2025, Your responsibility, your actions, their privacy	NUHT0000206

163	Data Breach Campaign communications and engagement plan	NUHT0000190
164	Data breach campaign draft posters	NUHT0000191
165	Email from Tom Watson to NUH re best practice on spot auditing dated 10 July 2025	NUHT0000202