|  |
| --- |
|  |
| **Version Number:** 1.5 | **Date of Next Review:** 1st February 2022 |
| IT Account Request Approval Form and Data Security and Confidentiality Agreement |
| Introduction and AimThis document is written in support of the Cardiff and Vale [Information Technology (IT) Security Policy](https://cavuhb.nhs.wales/files/policies-procedures-and-guidelines/corporate-policy/i-j-corporate-policy/1-14a-it-security-policy-pdf) and [Information Governance Policy](https://cavuhb.nhs.wales/files/policies-procedures-and-guidelines/corporate-policy/i-j-corporate-policy/cv-ig-policy-v4-pdf).Successful completion of this document will allow individuals that are not employees of Cardiff and Vale University Health Board and that meet a specific criteria to have a NADEX (computer log on) account that will allow them access to the Cardiff and Vale University Health Board (CAV UHB) network and appropriate IT systems. |
| ScopeThis document applies to non-fixed contracts, local government, agency, volunteers, temporary personnel including students, work placements/work experience **that** **need access to CAV UHB IT systems only.**Where the applicant **also** **requires access to or contact with Patients**, it is the CAV Sponsor’s responsibility to confirm if the applicant requires an Honorary Contract (HC).Cardiff and Vale University Health Board will issue honorary contracts to individuals who are not employed by the UHB, but who will come into contact with staff, patients or members of the public whilst carrying out work on the Health Board's premises. See <https://cavuhb.nhs.wales/staff-information/your-employment/honorary-contracts/>  |

# IT Account Request Process

# Guidance for completing the IT Account Request Approval Form

The following must be fully completed prior to submitting this form to **CV.IMT.Security@wales.nhs.uk****.**

Quote the **Applicant’s Name** and **IT support call job reference number** on all correspondence.

Incomplete forms will be rejected resulting in a delay in IT access.

1. The Cardiff and Vale University Health Board (CAV UHB) Sponsor has completed a **New Account Request** via the **IT Helpdesk**. Please include the **IT support call job reference number** in all correspondence.
2. The CAV Sponsor is responsible for ensuring all sections of this form are fully completed.
3. The Applicant has reviewed the document and signed Section 1\*
4. The Applicant’s Manager has reviewed the document and signed Sections 2 & 3\*
5. The CAV Sponsor has reviewed the document and signed Section 4\*
6. The fully completed form (and supporting documentation\*) is sent to **CV.IMT.Security@wales.nhs.uk**
7. Both the applicant and the applicant’s manager must keep a copy of the form submitted for their records.

**\*NB Typed signatures are** accepted where this form is accompanied with an email confirmation from the signatory confirming the document has been read, understood and accepted.

# IT Account Request Approval Form

|  |
| --- |
| **Section 1: Applicant Personal Details** (To be completed & signed by Applicant) |
| Title: Mr / Mrs / Miss / Ms / Dr / Prof **(delete as appropriate)** |
| Surname: |
| Forename: |
| Work Address: Postcode:  |
| Job Title: |  |
| Please provide brief details of the work the applicant will be undertaking in CAV UHB: |  |
| Employing Organisation or University: |  |
| Department: |  |
| Tel:  | Email:  |
| **Declaration (to be signed by the Applicant)** |
| I confirm:1. The information provided on this form is correct
2. I have read and understood the statements in the **Data Security and Confidentiality Agreement** below, and agree to adhere to the guidelines regarding the confidentiality of information within Cardiff and Vale University Health Board.
3. I will contact the IT Security Department immediately should my need for IT access cease prior to the expiry date
4. I also understand that any failure to adhere to these rules could result in action being taken against me.
 |
| Date: ..............................................................Print Name: .......................................................... Applicant Signature\*: ................ ................ ..................................... \***NB** if providing a **typed signature**, this document must be **accompanied with email confirmation** from the applicant that they have read and signed this document**.**  |

|  |
| --- |
| **Section 2: Reason for IT Account Request (please tick the appropriate box(es)****(To be completed by Applicant’s Manager)** |
| Will the applicant’s role require access to or contact with CAV UHB Patients?  | [ ]  **YES - DO NOT proceed with completion of this document**. Please complete the Honorary Contract process#. <https://cavuhb.nhs.wales/staff-information/your-employment/honorary-contracts/>#Where an exception to the Honorary Contract process exists please provide written confirmation from HR/Information Governance to confirm this Patient Facing applicant **DOES NOT** require an Honorary Contract.  |
| [ ]  **NO -** the applicant **only** requires access to CAV UHB IT systems – as specified in the logged IT Helpdesk Call reference below |
| The CAV UHB Sponsor must complete a **New Account Request** via the **IT Helpdesk**. Please provide the IT Support Call Job Reference Number: |  |
| Access to CAV UHB IT **systems** required (maximum 3 years)Start Date: End Date:The application / renewal must have a start and end date (maximum duration is 3 years)The IT Security Department must be informed immediately should the need for IT access cease. |

|  |
| --- |
| **Section 3: Applicant’s Manager Personal Details (substantive employment)****(To be completed and signed by Applicant’s Manager)** |
| Title: Mr / Mrs / Miss / Ms / Dr / Prof **(delete as appropriate)** |
| Surname: |
| Forename: |
| Work Address: Postcode: |
| Job Title: |  |
| Employing Organisation or University: |  |
| Department: |  |
| Tel:  | Email:  |
| **Authorisation (to be completed by Applicant’s Manager)** |
| As the applicant’s manager:1. I agree to take full responsibility for the day-to-day supervision of the above named individual and their work.
2. I confirm that the work they will be undertaking is appropriately approved and all relevant checks have been undertaken.
3. I will ensure that they are fully informed of the relevant [UHB policies e.g. Data Protection, Email Local Procedure, Internet User Local Procedure, etc.](https://cavuhb.nhs.wales/about-us/policies-procedures-and-guidelines/corporate-policies/)
4. I have read and understood the statements in the **Data Security and Confidentiality Agreement** below, and agree to adhere to the guidelines regarding the confidentiality of information within Cardiff and Vale University Health Board.
5. I confirm that I will inform the CAV UBH Sponsor and/or IT Security Department immediately should the need for IT access cease prior to its expiry date.
 |
| Date: ..............................................................Print Name: ..........................................................Manager’s Signature\*: ........................................... \*NB if providing a **typed signature**, this document must be **accompanied with email** confirmation from the both the Applicant and Applicant’s Manager that they have read and signed this document. |

|  |
| --- |
| **Section 4: Cardiff and Vale UHB Sponsor Personal Details** |
| Title: Mr / Mrs / Miss / Ms / Dr / Prof **(delete as appropriate)** |
| Surname: |
| Forename: |
| Job Title: | Hospital Site: |
| Dept: | Directorate: | Clinical Board: |
| Tel: | Email: |
| As the CAV UHB Sponsor:1. I agree to take responsibility to ensure the applicant receives full training and supervision of the above named individual and their work.
2. I confirm that the work they will be undertaking is appropriately approved and all relevant checks have been undertaken.
3. I will ensure that they are fully informed of the relevant [UHB policies e.g. Data Protection, Email Local Procedure, Internet User Local Procedure, etc.](https://cavuhb.nhs.wales/about-us/policies-procedures-and-guidelines/corporate-policies/)
4. I confirm that I will inform the IT Security Department immediately should the need for IT access cease prior to its expiry date.
 |
| Date: ..............................................................Print Name: ...........................................................CAV UHB’s Signature\*: ........................................... \*NB if providing a **typed signature**, this document must be **accompanied with email confirmation** from the both the Applicant and Applicant’s Manager that they have read and signed this document. |

|  |
| --- |
| **Section 5: IT Security Department** |
| Date Request Received: ......................................................................Actioned by: ............................................................... Date Actioned: ........................................................ |

# Data Security and Confidentiality Agreement

|  |
| --- |
| **Data Security and Confidentiality Agreement**(This applies to non-fixed Contracts, agency, local government, volunteers, temporary personnel including Students, work placements/work experience)  |
| In the course of your time working with *Cardiff and Vale University Health Board (the UHB)* you may have access to sensitive and confidential information concerning patients, staff, the business of the organisation and other third parties. Everyone has the right to expect his/her information to be dealt with the highest possible level of confidentiality. In dealing with this type of information you should work within the UHB’s policies and procedures (in particular the IM&T Security, Data Protection and the Confidentiality Code of Conduct). These can be found on the [UHB internet website.](https://cavuhb.nhs.wales/about-us/policies-procedures-and-guidelines/corporate-policies/)In addition to these policies, this document explains the UHB’s expectations with regard to confidentiality of information, what your responsibilities are, and what consequences a breach of confidentiality may be applied.**Confidentiality – General Guidelines*** Information which the UHB holds includes patient, clinical, financial, employee or contractual details. This is not a definitive list, and therefore if you have any doubts about the confidentiality of information it must be regarded as confidential unless you are advised otherwise by your supervisor/line manager. If your supervisor is not available then you should contact either the UHB’s Caldicott Guardian/Data Protection Officer or a member of the Information Governance Team.
* You must not use any personal, sensitive or patient identifiable information you come into contact with or as part of your duties, other than as part of your job role.
* You must not reveal or disclose personal, sensitive or patient identifiable information to friends or relatives.
* You must not discuss the patient with his/her friends of relatives without the patient’s consent.
* You must not discuss individual patients with another member of staff in patient areas.
* You must not reveal or disclose personal, sensitive or patient identifiable information to individuals, people making inquiries, or other agencies without the permission of your supervisor/line manager. (This includes not disclosing / discussing information on social network sites).
* Access to a patient’s medical record is restricted to relevant hospital staff dealing with the patient care.
* Enquiries from the press or police seeking information should be directed to your supervisor or a member of the Information Governance Team.
* The identity of all callers should be checked. Ask for a telephone number so that they can be called back by the person to deal with the enquiry.
* You must not download any information onto personal devices such as USB sticks, phones, cameras etc.
* You must not allow individuals to be identified during training or other health service activities.
* This duty of confidentiality continues to apply indefinitely to deceased patient information.
* All confidential records, including computerised material, documents and other papers, together with any copies or extracts thereof, made or acquired by you in the course of your placement shall be the property of the UHB and must be returned on the subsequent cessation of your time working with the UHB.
* This duty of confidence will continue indefinitely following completion/end of your placement.

**General Legal and Professional Principles**The Data Protection Act 2018, General Data Protection Regulations, Human Rights Act 1998 and the Common Law Duty of Confidentiality all refer to the protection of privacy and confidentiality. You will be required to adhere to this legislation at all times.**The Data Protection Act 2018** This covers the processing of personal data on living individuals held in any form, for example paper (health records) computer records, audio and video tapes. This act requires that data is 1) processed fairly and lawfully; 2) processed for a specified, explicit and legitimate purpose; 3) adequate, relevant and not excessive; 4) accurate and up to date; 5) not held for longer than necessary; 6) processed in a manner that ensures appropriate security of personal data.Patient information is defined under the Data Protection Act as “sensitive data” and additional specific conditions covering its use exist. Obtaining or disclosing such information without appropriate authority is a criminal offence.You should be aware that you will be personally liable for any contravention of the above legislation and that the duty of confidence lasts indefinitely. All requests for copies of information should initially be discussed with your supervisor/line manager or a member of the Information Governance Team.**The Computer Misuse Act 1990** This establishes three offences which refer to unauthorised access, either casually or for a more sinister purpose, to the modification of information and introduction of malicious programmes:1. It is an offence to knowingly cause a computer to perform any function with intent to secure unauthorised access to any programme or data held in any computer;
2. An offence under point 1 is committed with the intent to commit or facilitate a further offence, whether by the offender or by another person;
3. Knowingly to do any act which causes an unauthorised modification of the contents of any computer; to impair the operation of any computer; to prevent or hinder access to any program or data held and to impair the operation of the program or the reliability of the data.
 |

|  |
| --- |
| **Breaches of Confidentiality*** You must be aware that unauthorised access to, modification, or disclosure of information held by the UHB is strictly forbidden and attempts to do so will result in the immediate termination of your placement and/or even prosecution.
* In addition, serious breaches of confidentiality involving personal and sensitive personal informationmay result in legal proceedings being instigated under the Data Protection Act 2018.

Any breaches made by the applicant must be reported to the applicant’s manager and the CAV UHB Information Governance department immediately. |
| **Further Guidance**Any concerns you have in respect of the above issues should be raised with your supervisor/line manager (or the person you are reporting to), the Caldicott Guardian/Data Protection Officer or a member of the Information Governance Team. |
| **Acceptance**In signing this document I confirm I have read and understood the above statements and agree to adhere to the guidelines regarding the confidentiality of information within Cardiff and Vale University Health Board.I also understand that any failure to adhere to these rules could result in further action being taken against me. |