**Primary Care ICE account ID form**

**PLEASE FILL IN AND RETURN TO:**

**North Bristol:** gplinks@nbt.nhs.uk

**UHBristol & Weston:** [ice.support@uhbw.nhs.uk](mailto:ice.support@uhbw.nhs.uk)

PLEASE COMPLETE ALL BOXES

|  |  |
| --- | --- |
| **Surname:** |  |
| **First Name:** |  |
| **Title:** |  |
| **NHS Email address:** |  |
| **GP Practice(s):**  (List all of the GP Practices the individual works at) |  |
| **GP Practice National Code(s):**  (List all of the codes the individual works at to allow for a single access for all) |  |
| **Primary Care Network (PCN)**  (List all of the PCNs the individual works at to allow a single access for all) |  |
| **Generic Practice email address for correspondence**  **\*Please list addresses for all relevant practices\***  **This is a requirement to support communication regarding rejected requests.** |  |
| **ICE instance(s) required to connect to** | ¨ University Hospitals Bristol & Weston  ¨ North Bristol Trust  ¨ Remove user from practice |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **GPs (including locum). Please tick role below**  ¨ **GP (Locum)** ¨ **GP (Permanent)**   |  |  | | --- | --- | | **GMC number** |  | | **General Medical Practice** [**PPD Code**](https://faq.nhsbsa.nhs.uk/knowledgebase/article/KA-03100/en-us) |  | | **Permanent GP** | **Results returned to own workflow** | | **Locum GP** | **Results returned to specified GP. Please indicate below:**  **------------------------------------------------** | | **If the user is a LOCUM please provide end date**  The account will be inactive from this date | **END DATE:** | |

|  |  |
| --- | --- |
| **Nurses, Allied Health Professionals, Physician Associates and Clinical Pharmacists**  **Imaging requesting for Non Medical Referrers – please refer to the following process for additional steps**  [**REMEDY**](https://remedy.bnssg.icb.nhs.uk/adults/radiology-imaging/) **and** [**ALMC**](https://avonlmc.co.uk/guidance/radiological-imaging-for-non-medical-requesters/)  **Employed Role**  Please tick relevant box from list on the right. This will link to the most appropriate requesting entitlements on ICE | ¨ **Advanced Practitioner (Nurse)**  ¨ **Advanced Practitioner (Dietician)**  ¨ **Advanced Practitioner (Paramedic)**  ¨ **Advanced Practitioner (Pharmacist)**  ¨ **Advanced Practitioner (Physiotherapist)**  ¨ **Advanced Practitioner (Podiatrist)** ¨ **FCP Podiatrist**  ¨ **FCP MSK Physiotherapist**  ¨ **Clinical Pharmacist** ¨ **Dietician (pathology only)** ¨ **Paramedic** ¨ **Physician Associate (pathology only)** ¨ **Registered Nurse (pathology & radiology - not an ANP)**  ¨ **Registered Nurse (FSRH trained)**  ¨ **Registered Nurse (pathology only)**  ¨ **Nursing Associate (pathology only)** |
| **If the user is a LOCUM please provide end date**  The account will be inactive from this date | **END DATE:** |
| **Professional Registration number** (NMC/HCPC/GPhC or relevant governing body) |  |
| **Admin & Clerical will be given ‘Read Access’ only**  HCA – will be given ‘Read Access Only’ unless they are in an employed role that requires requesting | ¨ **HCA (view only)**  ¨ **HCA – Requesting role (pathology only)**  ¨ **Admin/Clerical roles (view only)** |

**PLEASE READ THE FOLLOWING AND CONTINUE TO THE END TO COMPLETE THE FORM**

**DO NOT SHARE YOUR PASSWORD WITH ANY OTHER PERSON**

Confidentiality of Personal Information and Personal Computer Software Misuse of Computer Act 1990

Under the Misuse of Computers Act 1990, a person is guilty of a criminal offence if they:

1. Gain, or attempt to gain, unauthorised access to a computer system.
2. Make any unauthorised alterations to software or data contained on a computer system.

All information about patients or staff is strictly confidential and must not be passed to any unauthorised person within or outside the Trust without prior consent of patients or staff. Protection of computerised data about individuals is now a requirement of the Law. The Data Protection Act 1998 lays down the following:

All persons that use information on a computer, or produced from a computer, have an obligation to see that it is not passed on in any unauthorised way. Surgery staff must not disclose any personal information obtained from computers, or any other computer output, in any way other than for discharging of their duties. If you are in any doubt, contact your supervisor BEFORE disclosing any information**.**

1. Purpose - The acceptable use policy highlights the user responsibility elements of the ICE security policy. It is a condition of the use of ICE applications that each user reads, understands and agrees to abide by the acceptable use policy.

2. Physical Security - Users are responsible for ensuring that:

Information is not displayed to individuals who do not need to know - this includes hiding (via screensavers or turning off displays) any activity they are undertaking, when approached by an individual who does not need to know information they have on screen.

They do not leave their desks without either logging out of the system, locking their PC (depending on the operating system they run) or using a password-controlled screensaver. If their PC is used for inappropriate activity recorded under their username, whilst they are away from their desk, it is their responsibility to prove they were not involved.

Their PC is protected from physical & environmental threats as far as possible, such as liquid spills or theft

3. Usernames & Passwords - All users will have been issued with their username and password, giving them appropriate access to systems and information for their role.

All users agree to:

Not to allow other people to use their account

Keep their password secret

Not write their password down

Use a password that is not obviously linked to them (i.e. partners name etc)

Not use consecutive parts of phrases in passwords (Rover1 should not be replaced with Rover2) A good password methodology is to use the first letters of a phrase - (We Have A Boat That Is Blue) - WHABTIB.

4. Email Addresses – When registering for ICE users are requested to enter a valid and appropriate email address. This should bean NHS email address, either for their organisation or an NHS.Net email address. The ICE supports access for additional supporting organisations and as such these are also supported for email address validation. Personal email addresses should not be used (e.g. Hotmail, Gmail). Email addresses should also be unique to the user; duplicate email addresses for different user are not permitted. Email accounts which are shared for business purposes should not be used for registration of ICE.

5. Best Practice & Legal requirements - It is the responsibility of every user, in conjunction with their employing organisation, to ensure they are aware of local Information Security Policies, to know who their Data Protection Officer and Caldicott Guardian are and be familiar with:

Local codes of conduct for computer system use

Confidentiality clauses within their contract of employment or professional registration

Security procedures relevant to their work & environment

Best practice in maintaining security of computer systems (e.g. Passwords, clear screens etc)

Best practice in handling confidential information in line with Caldicott principles

Caldicott Principles:

Justify the purpose of collecting, using and sharing the information

Only use when absolutely necessary

Use minimum required information

Access only on a need to know basis

Understand your responsibilities

Understand and comply with the law.

Users will ensure that:

Any activity they undertake on ICE application will be in respect of the official business of their employing organisation and not for personal gain or with malicious intent.

They will only access information on patients where they can justify a need to know for the purpose of treatment/care (or administration of) that patient.

They will only provide information they have accessed via the system(s) to others when they are sure of the recipient's purpose and need to know.

Any printouts or other form of copying information from the systems that they undertake will be handled appropriately and all possible steps to protect the information will be undertaken, in line with organisational policy.

User activity will be audited and any abuse (suspected or otherwise) will be traced and reported to the employing organisation, to be investigated and dealt with under the appropriate HR disciplinary policy.

the event of suspected misuse or breach of confidentiality, the 'system owners' reserve the right to remove any user's access either temporarily or permanently.

When registering ICE, users will be required to view and agree to this Acceptable Use Policy. Completion of their registration will confirm that they accept these terms. During the use of the system(s) users will have the opportunity to access both this Acceptable Use Policy and the overarching Information Security Policy.

6. Patient Consent - Unless patients are specifically asked for their consent, then it can only be implied. Due to the nature of the applications and their use in the process of delivering care, in most cases patients consent can be implied, or is a condition of receiving treatment. However for this to be valid, patients must be informed and understand the process. Where possible a user will gather consent from the patient to access their information (i.e. patient present).

7. Unused Accounts - If an account has not been used for a set period the users account will be suspended and it will not be possible for them to log in. It will be reactivated upon request to the appropriate administrator. If an account has not been used for a further set period the account will be deleted and the user will have to re-apply.

8. Changes to user information - Managers will require to contact the Digital Services Service Desk Tel 0117 3423939 option 2 With any changes to their staff roles or when they leave the organisation.

9. Protection from 'Malicious' Software - All users will ensure that their actions do not expose their PC or the ICE applications to any threat from virus software etc. Users with any concerns over how this should be achieved must contact their local IT support.

10. Business Continuity - Each user shall ensure they are aware of the appropriate 'fall back' procedures to be put in place if there is a system failure, to ensure continuity of service. These will be highlighted during training. In the event of system failure the user shall attempt to establish the reason for failure, this will fall into one of three categories, listed below:

Local - failure of PC(s), failure of organisational network, failure of organisational NHSnet connection.

Host - failure of application server, failure of host network, failure of NHSnet connection

Inter-Organisational - failure of network communications (part or full) of NHSnet. This is the responsibility of the commercial providers of NHSnet.

First point of contact following any failure will be the local support facilities (helpdesk). They will then pass on appropriately. In situations whether there is no local support other support arrangements will be implemented.

11. Specific application elements - This policy covers general uses of the ICE application. However where appropriate an application will have its own requirements. These will be included in the appendices to this document.

12. Management arrangements - This policy should be in line with the user elements of any organisational Information Security Policy. It is designed to complement existing policy and not replace it. As developments progress with the use of 'ICE’ for clinical and operational functions, this policy will be revised.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| I am fully aware of my practice or PCN policies for the use of electronic systems and I have read and understand the terms of the policies and supporting documents appropriate to my employed role and agree to abide by them. | | | | | |
| Signature | | | Date | | |
| ICE password (assigned and emailed to user) | | PACS ID | | PACS password | |
| I have provided or signposted all relevant documents, policies and protocols to the individual above and I confirm that the practice has appropriate governance and procedures in place to support this activity. In the case of working across multiple practices **please ensure each relevant Practice Manager signs this document and indicates agreement for results to be returned to the registered clinician.** | | | | | |
| Practice Name | Practice Manager Name | | Practice Manager signature | | Do you agree for the results be returned to the individual clinician?  Please indicate YES or NO |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |