CODE of CONDUCT in RESPECT of CONFIDENTIALITY

PROVIDING A CONFIDENTIAL & SECURE ENVIRONMENT FOR ORGANISATIONAL INFORMATION

The Trust is committed to providing a robust Information Governance (IG) framework and to provide clear direction, approach and support. The NHS IG Initiative combines both NHS & legal requirements governing how such records & information are handled.

This policy should be read in conjunction with supporting IG Policies.

Who is included: This policy applies to everyone who works in the Trust regardless of hours or base. This includes, students, substantive and temporary staff, those on honorary contracts, NBT eXtra staff, medical staff, volunteers and those appointed to the Trust through redeployment.

Definition:

The document is the development of effective systems management procedures & practices whereby IG requirements are met & established as an integral part of the Trust's business & culture

The IG Framework encompasses the following NHS& legal requirements:

- **Data Protection Act 1998, Common Law Duty of Confidentiality, Caldicott requirements, Human Rights Act 2000**
- **Computer Misuse Act 1998, ISO/IEC 27002:2005 Information Security Standards**
- **Freedom of Information Act 2000, Records Management: NHS Code of Practice, Public Records Act 1958**
- **To maintain competence to the required standard e.g. IG Toolkit, Care Quality Commission (CQC) standards and NHS Litigation Authority (NHSLA) risk Management Standards.**

Purpose

All employees, including Temporary Staff, Students, Volunteers and Locums, working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 1998 and, in addition, for health and other professionals through their own professions Code(s) of Conduct.

This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records.

It should be noted that employees also come into contact with non-personal identifiable information which should also be treated with the same degree of care e.g. business in confidence information such as patient referral letters, discharge summaries, waiting lists data, consultants work loads, clinic lists.

Disclosure and sharing of personal identifiable information is governed by the requirements of Acts of Parliament and government guidelines.

The principle behind this Code of Practice is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of North Bristol Trust's security systems or controls in order to do so.

This Code of Conduct has been written to meet the following legal requirements: -

- Data Protection Act (1998)
- Computer Misuse Act (1990)
- Human Rights Act (1998)
  - (Particularly Article 8, the Right to Respect for Private and Family Life)
- The Copyright Designs and Patents Act

This Code of Conduct has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements.

1 Information Governance Clauses within Employment Contracts

The Trust needs to ensure that those undertaking work on behalf of the Trust do so in a lawful manner and meet all appropriate Information Governance (IG) requirements.

It is vital therefore that the contracts or permanent, temporary and locum staff contain clauses that clearly identify responsibilities for confidentiality, data protection and information security.

The Trust must take reasonable steps to vet staff and provide IG training, or request appropriate training is undertaken before permitting them to access the systems and information.

2 Screening

Screening criteria will be established for jobs, contracts and appointments to ensure that candidates conform to legislation and special requirements (such as security clearance for some positions).

The Human Resource department will be responsible for defining the criteria and ensuring that screening checks are carried out.

Written procedures have been established to detail these responsibilities. Typically, checks are carried out to verify references, qualifications, identity, criminal record and employment record.

3 Terms & Conditions of Employment

Employment terms should address the following criteria:

- Legal responsibilities, including confidentiality and non-disclosure clauses;
- Information Security responsibilities, including encryption, home working and remote access (where applicable)
- Records management and Information Quality responsibilities
- Actions to be taken if the employee, contractor or third party user disregards the Trust's information governance standards

4 Roles and Responsibilities

The Trust must comply with all aspects of the law that are concerned with the processing or personal data. This includes legislation (Acts of Parliament), regulations and common law duties.

Health & Social Care Professionals must meet the codes of practice of their professional bodies and each individual (employees, contractors, locums etc.) has a personal responsibility to comply not only with the law but also with provisions set down by their contracts of employment supported by the Trusts guidelines and documented best practices and policies.

Whilst clearly identifying the responsibilities will not automatically absolve the Trust of all blame, it will be of assistance should an individual deliberately or recklessly breach the law.

Therefore all Information Governance responsibilities for those undertaking work on behalf of the organisation will be defined and documented in contracts and supported by this Code of Conduct.

4.1 Management Responsibilities

Individuals must be made aware of their responsibilities through documentation, training and awareness sessions, including induction and other awareness materials.

In the case of dealing with sensitive information, wherever practicable the Trust will ensure that training is provided before access is granted.

Training, education and awareness material will be regularly updated.

4.2 Termination or Change of Employment Responsibilities

There are written procedures for managing changes to staff employment, issued by the Human Resource department. Confidentiality and other responsibilities are included in any termination documentation.

All assets (equipment, documentation, smartcards, id badges, office keys etc) issues to employees, contractors and third party users is recorded in an up to date asset register. Procedures are in place for the return of assets on termination of a contract and where applicable on change of employment within the Trust.

Access rights include physical and logical access gained through keys, ID cards, passwords etc. Procedures are in place to ensure an assessment is carried out to establish what access rights are required and when access rights should be withdrawn; e.g. employee working a month's notice may no longer require laptop use but will need to use a range of systems until the last day

of employment.

In the case of management terminating employment or a contract with a third party, the Trust may terminate all access immediately and will ensure that all accounts are locked and passes/ID cards invalidated.

Similarly, a disgruntled employee or contractor's employment be terminated, management will take actions to ensure information and facilities are not misused, corrupted or destroyed.

5 Detailed Provisions

5.1 Confidentiality of Information

All employees are responsible for maintaining the confidentiality of information gained during their employment by North Bristol Trust.

5.2 Definition of Confidential Information

Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored; e.g. information may be held on paper, floppy disc, CD, computer file or printout, video, photograph or even heard by word of mouth.

It includes information stored on portable devices such as laptops, palmtops, mobile phones and digital cameras.

It can take many forms including medical notes, audits, employee records, occupational health records etc. It also includes company, (Trust) confidential information.

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode (part or full), and date of birth, NHS Number, National Insurance Number.

Please note even a visual image (photograph) is sufficient to identify an individual.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation; e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancies.

During your duty of work you should consider all information to be sensitive, even something as a patient name and address.

The same standards should be applied to all information you come into contact with.

5.3 Requests for Information on Patients or Members of Staff

- Never give out information on patients or staff to persons who do not "need to know" in order to provide health care, treatment or employment information.

- All requests for identifiable information should be on a justified need and some may also need to be agreed by the Trust's Caldicott Guardian and/or Information Governance Manager.

All expectations to this rule may require you to get written consent from the patient or member of staff in advance.

If the patient is unconscious and unable to give consent, consult with the health professional in charge of the patient's care.

If you have any concerns about disclosing/sharing patient or staff information you must discuss with your manager and if they are not available, someone with the same or similar responsibilities.

If you cannot find anyone to discuss the issue with you should take the callers details and ring them back when you are satisfied the disclosure or information can take place.

5.4 Telephone Enquiries

If a request for information is made by telephone:

- Always check the identity of the caller and whether they are entitled to the information they request
- Take a number, verify it independently and call back if necessary.

Remember that even the fact that a patient is in hospital, a patient of the hospital or a member of staff, is confidential.

If in doubt consult your manager or refer to the Guidance leaflet, 'Handling Phone Calls…'.

5.5 Requests for Information by the Police and Media

With respect to the Police:

- Requests for information from the Police should always be referred to the consultant or health professional in charge of the

- patient's care, or to the appropriate senior manager, the on-call director (if out of hours) or the Trust's Head of Information Governance.

With respect to the Media:

- Do not give out any information under any circumstances.

Requests for information from the media or from the Police that are media-connected should always be cleared through the Press Office.

5.6 Disclosure of Information to Other Employees of North Bristol Trust

Information should only be released on a "need-to-know" basis.

- Always check the member of staff is who they say they are
- This can be achieved by checking the employee's ID badge and/or their internal them any information extension number or bleep number prior to giving
- Check whether or not they are entitled to the information
- Do not be bullied into giving out information

If in doubt, check with the consultant/doctor in charge of the patient's care or with your line manager.

5.7 Carelessness

- Do not talk about patients or staff in public places or where you can be overheard.
- Do not leave any medical records or confidential information lying around unattended
- Make sure that any computer screens, or other displays of information, cannot be seen by the general public

5.8 Faxing

Remove person identifiable data from any faxes unless you are faxing to a known secure and private area (known as 'Safe Havens')

- Faxes should always be addressed to named recipients
- Always check the number to avoid misdialling and ring the recipient to check that they have received the fax
- If your fax machine stores numbers in the memory, always check that the number held is correct and current before sending sensitive information

6 Use of Internal and External Post

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient.

This means personal information/data should be addressed to a person, a post holder, a consultant or an legitimate Safe Haven, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or a team leader.

Internal mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. 'Confidential' or 'Addressee Only', as appropriate.

External Mail must also observe the rules.
Special care should be taken with personal information sent in quantity, such as case note's, or collections of personal records on paper, floppy disc or other media. These should be sent by Recorded Delivery or by NHS courier, to safeguard that these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain receipt as proof of delivery e.g. patient records to a solicitor.

Case note's and other bulky material should only be transported in the approved boxes and never in dustbin sacks, carrier bags or other containers.
These containers should not be left unattended unless stored, waiting for collection, in a secure area e.g. ideally locked. The containers should only be taken and transported by the approved carrier.

Blood samples etc. should also only be transported within the correct authorised containers and should not be left lying around within ward areas or when they have been delivered to the laboratory.

7 Storage of Confidential Information

Paper-based confidential information should always be kept secure and preferably in a room

that can be locked and in some cases alarmed when unattended, particularly at nights and weekends or when the building / office will be un-occupied for a long period of time.

PC-based information should not be saved onto local hard drives or onto removable media, but onto the Trust's network. Floppy discs and other media should also be kept in locked storage.

8 Disposal of Confidential Information

When disposing of **paper-based person identifiable** or confidential information always use either the 'Confidential Waste' wheelie bins or the 'Confidential Waste' nylon sacks. Keep the waste in a secure place until it can be collected.

Computer printouts should either be shredded or disposed of as paper-based confidential waste.

CDs containing confidential information must be either reformatted or destroyed. Computer files with confidential information no longer required must be deleted from both the PC and the server if necessary.

Computer hard disks are usually destroyed/disposed of by IT Services, by any means they see fit.

This is to ensure all information is deleted from the disk, as even by re-formatting it is possible to gain access to the original data.

X-Rays that are no longer required must be disposed of in the correct manner.

These must not be disposed of in waste bins, other confidential waste disposal method, for example sacks, shredders, or in clinical waste sacks.

The disposal and destruction of x-rays can cause a threat to the health of anyone trying to destroy them unless the correct method is used – and this is only available by specialist suppliers.

9 Emailing Confidential Information

Please seek advice from your Head of Information Governance if you have the need, or possible need, to e-mail person identifiable information.

The e-mail transmission internally over the Trusts network can pose serious risks to confidentiality and should not be considered a secure way to communicate, unless it is essential to the delivery of care. In which case strict principles should always be followed.

Patient identifiers should be removed wherever possible and only the minimum necessary information sent, this may be considered to be the NHS Number but no name or address.

This in itself can pose problems as the wrong number may be typed.

Special care should be taken to ensure the information is sent only to recipients who have a "need to know"; always double check you are sending the e-mail to the correct person(s).

External transfers should only take place to persons with access to NHSnet.

Under no circumstances whatsoever, should any type of patient identifiable information sensitive or confidential information about any other person be e-mailed to persons who only have Internet access. Due to its insecure nature any information transmitted over the Internet should be considered to be in the public domain.

10 Working at Home

Trust Policy does not allow identifiable information to be used other than within NHS premises.

However, it is sometimes necessary for employees to work at their own home.

If you need to do this you would first need to gain approval from your manager.

If they agree you would need to ensure the following are considered and remember that there is personal liability under the Data Protection Act 1998 and your contract of employment for breach of these requirements:

- Ensure you have authority to take records. This will normally be granted by your line manager.
- If you are taking manual records please ensure there is a record that you have these records, where you are taking them and when they will be returned.

This is particularly important for patient records.

A tracer card system or electronic tracking system should suffice, if there is not one a manual system should be in place.

Under no circumstances whatsoever, should any

type of patient identifiable information, sensitive or confidential information about any other person be e-mailed to persons who only have Internet access.

Due to its insecure nature any information transmitted over the Internet should be considered to be in the public domain.

- Ensure any personal information in manual form e.g. patient/staff files, or electronic format e.g. floppy discs/CDs, are in sealed containers prior to them being taken out of the Trust.
- Make sure they are put in the boot of the car or carried on your person while being transported from your work place to your home.

While at home you have personal responsibility to ensure the records are kept secure and confidential.

This means that no other members of your family and/or friends/colleagues must not be able to see the content or outside folder of the records.

- You must not let anyone have any access to the records.

If you take home computer records on a floppy disc or CD you must ensure all of the above apply. In addition you must ensure if you are putting information onto your own PC that you take the information off again when you have finished your work.

- Other family members must not be able to access this information.

When taking your records back to work this must be carried out as above, in secure containers etc. For manual records they should be logged as being back within the Trust.

For computer records on floppy disc/CD these MUST be virus checked before being loaded onto any of the Trusts systems – especially any that can be accessed by the network.

11 Copying of software

All computer software used with the Trust is regulated by license agreements. A breach of the agreement could lead to legal action against the organisation and/or the offender (member of staff).

It is important that software on the PCs/systems used for work purposes must not be copied and used for personal use. This would be a breach of the license agreement.

12 Confidentiality of Passwords

Personal passwords issued to you or created by employees should be regarded as confidential and those passwords must not be communicated to anyone.

- Passwords should not be written down
- Passwords should not relate to you or the system being accessed.

You will be given more information about passwords control and format when you receive training and/or password.

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees.

Any attempt to breach security should be immediately reported to the IT Security Officer and may result in a disciplinary action and also a breach of the Computer Misuse Act 1990 and/or the Data Protection Act 1998, which could lead to criminal action being taken against you.

If you are concerned that a colleague may be breaching security or confidentiality you may raise this under the Trust's 'Raising Concerns About Healthcare Services' Policy which, ensures your confidentiality will be respected and gives you advice and guidance on how to raise your concern.

13 Abuse of Privilege

It is strictly forbidden for employees to look at any information relating to themselves, family, friends or acquaintances unless they are directly involved in that patient's clinical care or with the employees administration on behalf of the Trust.

Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

14 The NHS Care Record Guarantee

The Care Record Guarantee sets out 12 high level commitments for protecting and safeguarding patient information, particularly in regard to: patients' rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing

information will be made.

The following commitments in the Guarantee map directly to the requirements set out in the Information Governance Toolkit.

Commitment 3
We will not share information (Particularly with other government agencies) that identifies you for any reason, unless:

- You ask us to do so;
- We ask and you give us specific permission;
- We have to do this by law;
- We have special permission for health or research purposes; or
- We have special permission because the public good is thought to be of greater importance than your confidentiality

If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS confidentiality code of practice and other national guidelines on best practice.

Commitment 4
Under current law, no-one else can make decisions on a person behalf, about sharing health information that identifies that person.

At the moment the only exceptions to this are parents or legal guardians, or people with powers under law, for example, that relating to mental health.

As of October 2007, individuals can appoint someone to have as lasting power of attorney to make decisions for them if they lost the ability to make decisions for themselves. Individuals can decide what rights that person has in making decisions about their care record.

If no person is appointed, a senior healthcare professional involved in the care may consider it to be in your best interests to share information.

This judgement should take account of the views of the relatives and carers and any views the individual may have already recorded.

For medical research or other purposes, the Patient Information Advisory Group can give special permission to share any health information that could identify an individual.

Commitment 5
Sometimes an individual's healthcare will be provided by members of a care team, which might include people from other services, such as social services or education.

The Trust must inform the individual if this is the case.

When it could be best for your care for the Trust to share health information with organisations outside the NHS, the Trust will agree this with the individual before hand.

If the individual does not agree, the possible effect this may have on the individual's care and any alternative available will be discussed with the individual.

Commitment 6
Usually and individual can choose to limit how the Trust shares the information in the electronic record.

In helping an individual decide, the healthcare professionals will discuss how this may affect the Trusts ability to provide the appropriate care and treatment and any alternatives available.

Commitment 9 We will make sure, through contract terms and staff straining that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work.

Organisations under contract to the NHS must follow the same policies and controls as the NHS does.

15 Disclosure of Information

Staff will be informed of the system contract terms and process currently in place that ensure personal is not inappropriately disclosed, e.g. Trust procedure for answering telephone queries, or information sharing protocols that set out the terms on which personal information may be shared with an external organisation.

Guidance will also be provided on the avoidance of inadvertent disclosure caused by discussion of Patient details in inappropriate venues, e.g. staff canteen, in the lift, on the bus etc.

Staff will be fully aware that action will be taken when records are deliberately looked at without authority, both electronic and paper.

This will include disciplinary action, ending a contract, firing an employee, or bringing criminal charges.

Staff should also be aware that even where there is a genuine reason to disclose personal information this will not often require the whole of the patients record to be disclosed.

This code should inform staff of where to seek further assistance on a disclosure issue.

Where a disclosure is required, the Caldicott Principles should be applied;

The Caldicott Principles
Principle 1 - Justify the purpose for using confidential information

Principle 2 - Only use it when absolutely necessary

Principle 3 - Use the minimum that is required

Principle 4 - Access should be on a strict need to know basis

Principle 5 - Everyone must understand their responsibilities

Principle 6 - Understand and comply with the law

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

16 Use of Personal Information for Purposes Other than Healthcare

There may be occasions when the Trust wishes to use patient information it has collected for the purpose of providing treatment for another purpose, e.g. to a hospital chaplain.

To meet the legal requirements of the Data Protection Act 1998 and common law, the Trust should ensure that there are procedures in place to gain specific informed consent to use the information for secondary purposes.

The Trust must also ensure that staff are aware of a patient's right to restrict disclosure of their personal information and as far as possible ensure that this right is adhered to and respected.

Staff must be aware that possible disciplinary procedures may be invoked for failure to respect patients' rights.

When a patient provides or is otherwise the source of confidential information relating to their medical condition, the purpose is to receive treatment and related services for that condition.

Patients must still be made aware of who will see information about them in order to provide treatment and care, their consent to their information being used in this way can be implied.

However, patients retain the right to restrict disclosure of their confidential information, i.e. they have explicitly declined to allow information to be shared; this means that no one can make decisions about sharing this information on the patients behalf.

There are exceptions to this for patients or legal guardians or people with powers under the mental health law, e.g. the Mental Health Capacity Act 2005.

Before sharing personal information about a person lacking capacity, the information holder should consider the following questions;

- Is the person asking for the information acting on behalf of the person who lacks capacity?
- Is disclosure in the best interest of the person who locks capacity?
- What find of information is being requested?

The patient has the right to change their mind about a disclosure decision at any time before the disclosure is made, and can do so afterwards to prevent further disclosures where an activity requires a regular transfer of patient information.

Consent cannot be implied for purposes other than healthcare. Non healthcare purposes could include disclosure to the:

- Police
- Government departments other than the Department of Health
- Courts etc.

In most cases, patients should be asked for their explicit consent for information to be shared for non-care purposes.

However, there are certain circumstances under

which information can be disclosed for non-care purposes without seeking explicit consent or where the consent has been sought but refused.

These circumstances are:

- The disclosure is required or permitted by law
- There is a robust public interest in disclosure e.g. where failure to disclose would put someone else at risk

16.1 Required or permitted by law

Disclosure may be required by Court Order or under an Act of Parliament, e.g. there is legislation requiring that certain confidential information be disclosed to the Health Protection Agency for monitoring and controlling disease

Disclosure is also permitted under:

- Section 60 of the Health & Social Care Act 2001, now section 251 of the NHS Act 2006.

Applications to use Section 251 powers were previously considered by the Patient Information Advisory Group (PIAG) but will now be considered by the Ethics and Confidentiality Committee of the National Information Governance Board (NIGB).

16.2 Public Interest

Decisions about whether a disclosure is in the public interest should only be taken by senior members of staff such as the Caldicott Guardian.

Legal advice should be sought where necessary, but ultimately, the courts may have to decide whether a disclosure is or is not in the public interest.

16.3 Patient's Right to Restrict Disclosure of Personal Information - What to think about

- When and how consent should be obtained
- The basic premise that patients have the right to choose whether or not to agree to the use or disclosure of their personal information
- The right of patients to change their decision about a disclosure before it is made
- Who should obtain consent for the further purpose
- Where and how consent or dissent should be recorded
- Answering patients questions about including how to provide information about the consequences of non-disclosure to patients in a non-threatening, non-confrontational manner
- How often should this be reviewed
- Exemptions to the requirement for consent – public interest, legally required and section 60 of the Health & Social Care Act 2001, now section 251 of the NHS Act 2006.

17 Non-Compliance

Non-compliance with this code of conduct by any person employed by the Trust may result in disciplinary action being taken in accordance with the Trust's disciplinary procedure, and could lead to dismissal for gross misconduct.

To obtain a copy of the disciplinary procedures please discuss with your line manager or the Human Resource Departments.

17.1 Amendments

This code will be amended as necessary to reflect the Trust's development of policies and procedures and the changing needs of the NHS.

18 Equality Impact Assessment

The Trust's vision is to have in place a sustainable people driven service system of care which is best of class, and values based on hope inspiring environments and embracing diversity.

The Trust will ensure that all staff and service users, carers and visitors to the Trust are treated with dignity and respect, and no individual is treated differently on the grounds of their race, gender, disability, age, religious belief or their sexual orientation.

PLEASE RETAIN FOR YOUR INFORMATION

Current Version:	v6
Date of Original Issue:	1st December 2004
Date ratified:	September 2015
Policy Review Date:	September 2018
Main Author:	Head of Information Governance
Committee Approved:	Information Governance Committee

IG Policy documents will be reviewed and updated at not more than 3 yearly (36 months) intervals in accordance with *CO1 'Policy for the Development & Management of Trust Procedural Documents'*

Minor changes as necessary will be agreed by a quorate of the Information Governance Committee and the IM&T Security Group.

FINDING OUT MORE…

For further information on the Trust's Information Governance Management Framework agenda & Policies please speak to your Manager, or refer to the Head of Information Governance.

For more information please refer to:

http://sharepoint/sites/cec/MAINpolicies/IMT%20Policies/Forms/AllItems.aspx

Your personal responsibility concerning security and confidentiality of information (relating to patients, staff and the organisation).

During the course of your time within North Bristol NHS Trust you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of North Bristol Trust. This condition applies during your relationship with North Bristol Trust and when the relationship ceases.

Confidential information includes all information relating to North Bristol Trust and it's patients and employees. Such information may relate to patient records, telephone enquiries about patients or staff, electronic databases or methods of communication, use of fax machines, hand-written notes made containing information etc. If you are in doubt as to what information may be disclosed, you should check with your Information Governance Manager.

The Data Protection Act 1998 regulates the use of computerised information and paper records of identifiable individuals (patients and staff). North Bristol Trust is registered in accordance with this legislation. If you are found to have made an unauthorised disclosure you may face legal action.

I understand that I am bound by a duty of confidentiality and agree to adhere to this Code of Conduct and the requirements of the Data Protection Act 1998.

PRINT NAME: . . . . . .

SIGNATURE: . . . . . .

DATE: . . . . . .

On Behalf of NORTH BRISTOL NHS TRUST

WITNESS/MANAGERS NAME: . . . . . .

SIGNATURE: . . . . . .

DATE: . . . . . .