Belfast Health and Social Care Trust

Non-Trust Staff Confidentiality Agreement

Updated: 25 January 2021 v1.0

1. Introduction

In agreed circumstances, the Belfast Health and Social Care Trust ('the Trust') will provide access to its premises, electronic systems and/or patient/service user information, to external organisations or individuals ('third parties'). In these circumstances, a confidentiality agreement must be completed and signed by the third party. This agreement confers responsibility to the third party for any detriment, distress or damage caused by their behaviour by the third party, which leads to a loss, theft or damage to the personal data /sensitive personal data, held by the Trust. The Agreement can be signed by any manager, who has sought approval from the relevant manager in section 2 and must be retained for one year by the signing manager.

2. Third Parties

This agreement outlines the expectations and conferred obligations as detailed within data protection legislation and the Trust's data protection and confidentiality polices.

It is generally accepted that third parties will be non-HSC organisations/employees who are granted limited access to Trust information and do not have contractual terms to cover the access. This Agreement is applicable to the following third parties (but please note this is not a definitive list):

- Any ICT or telecom contractor (approved by an ICT Manager) who requires access to a Trust IT system.
- Any facilities or building contractor (approved by an Estates Manager) who will be accessing Trust premises.
- Any student/work placement (paid or unpaid) or volunteer who will be accessing Trust premises and/or patient/service user information (HR Manager/Service Manager approval is required).
- Any external panel member required for a Serious Adverse Incident Review (Senior Governance Manager approval from commissioning Directorate is required).
- Any external training providers or HR-appointed individuals
- Any individual required to complete audit, consultative or investigative/review work for the Trust (and where approval has been granted by the relevant Head of Service and above).
- Where there is no employment contract, this agreement may be used for agency and locum staff.

3. Alternative Third Party Arrangements

This Agreement is intended for one-off or limited and time bound access to Trust premises or information systems. It is not to be used in place of existing Trust processes, where the following may apply:

- Data Access Agreement (providing specific access to Trust data by external organisations for mutual benefit, with a lawful basis).
- Data Sharing Agreement (for routine and defined sharing between the Trust and another organisation/groups of organisations).
- Memorandum of Understanding (for wider sharing of information across broad categories or areas of mutual interest).

- Contract (a defined legal agreement which may permit further use of the information).

For further information on the above, please contact the Trust's Information Governance Department or Contracts Department.

4. Confidentiality of Trust Information

The Trust is entrusted with the sensitive information of patients and service users, who access its services each day. In the course of daily business this information is discussed, electronically sent, electronically/manually recorded, displayed and printed/posted – all of which is bound by confidentiality. This confidentiality comes from legislation (the Data Protection Act 2018, the UK General Data Protection Regulation and the Network Information Systems Directive); from case law (Enduring Duty of Confidentiality); Trust policies and; any professional obligations conferred upon Trust employees.

All third parties must ensure and accept that confidentiality extends to the following:

- Viewing of any confidential information (in paper or electronic form) relating to staff, service users or patients.
- Any conversations within the Trust where patient, staff or service user information is discussed or shared.
- All overheard conversations or inadvertent contact with/sight of confidential information, eg whiteboards, sign-in books etc).
- Any business sensitive information (in paper or electronic form), which is disclosed or discussed in the presence of a third party.
- Any sightings of patients/service users or their families (known to the third parties) whilst attending services within the Trust.
- Any personal information (not related to business information) relating to employees of the Trust.

The Trust is the 'data controller' for all personal data held by the Trust. As such, this information belongs to the Trust and not the patient, therefore the Trust will take appropriate action against any breach of its information, by a third party.

5. Requirements for Third Party (Organisation)

The Trust expects all third party organisations to satisfy the following conditions:

- Third party organisations must ensure their staff have an understanding of data protection responsibilities (either through training or policies) and these can be evidenced, if required.
- Each organisation must provide the Trust with an escalation process, with full contact details, for any issues or incidents relating to breaches of security or confidentiality.
- Each organisation must indemnify the Trust against any loss that the Trust incurs under data protection legislation that is caused by the organisation, whether authorised or unauthorised.
- All information generated by the organisation or its employee (via the Trust's manual/electronic systems), remains the property of the Trust and may be disclosed or used by the Trust, where the disclosure is deemed legitimate.
- The organisation must not take copies, remove or retain any electronic/manual

information, unless specifically agreed by the Trust.

- The organisation must not engage any sub-contractors without prior written agreement from senior Trust staff (see section 2).
- Confidentiality endures after the organisation has completed its interaction with the Trust and will remain in place, indefinitely.
- The organisation must be registered with the Information Commissioner's Office and provide assurance that there is no legal issue, potential concern or obstruction, to undertaking the proposed work within the Trust.
- The organisation will notify the Trust immediately if there is a data breach or a change in the agreed working arrangements.
- Any transfer of information (manually or electronically) and the method of transfer must be approved by senior staff within the Trust (section 2).
- Where information is transferred it must be kept secure and in line with Trust policies (section 8).
- All ICT equipment and devices belonging to the Trust must be returned directly to the appropriate Trust manager and it is the third party's responsibility to arrange and ensure the equipment/devices are safely returned.

6. Requirements for Third Party (Individual)

The Trust expects all individual third parties, to agree and ensure the following:

- Have previously completed data protection/information governance training and/or participate in data protection training provided by the Trust (if required).
- Confidentiality will endure after the individual has completed their interaction with the Trust and will remain in place, indefinitely.
- All information generated by the individual (via the Trust's manual/electronic systems), remains the property of the Trust and may be disclosed or used by the Trust, where the disclosure is deemed legitimate.
- The individual must not take copies, remove or retain any electronic/manual information, unless specifically agreed by the Trust.
- The individual will notify the Trust immediately if there is a data breach or they witness any incident or concern, during their time in the Trust.
- Any transfer of information (manually or electronically) and the method of transfer must be approved by senior staff within the Trust (section 2).
- Where there is agreement to transfer or retain information, it must be kept secure and in line with Trust policies.
- All ICT equipment and devices belonging to the Trust must be returned directly to the appropriate Trust manager and it is the third party's responsibility to arrange and ensure the equipment/devices are safely returned.

7. Freedom of Information Act 2000

The Freedom of Information Act (FOIA) applies to all of the Trust's activities/functions and will include the information generated or collected from the activities and functions. The third party shall accept and support the Trust's obligations under the FOIA by ensuring all relevant records are retained. The Trust may have to disclose information about an organisation or individual, in response to a request under the FOIA, but will (where appropriate) inform the third party ahead of the disclosure.

The FOIA does permit some exemptions to the release of information and if the Trust decides that an exemption is applicable, it will withhold the information but will not inform the third party.

8. Trust Policies

The following policies must be complied with, before the third party commences with the Trust or accesses Trust information / systems:

- Policy on Data Protection and Protection of Personal Information
- ICT Security Policy
- Social Media Policy

For access to particular service areas/premises or Trust information systems, the following additional policies or procedures must be reviewed:

Policy/Procedure name	Applicable area

In the event of a suspected data breach by the third party, the Trust will assess the incident and decide if it is reportable to the PSNI and/or the Information Commissioner's Office. In these circumstances, the Trust will present this document as an assurance that the third party is aware of the relevant polices.

9. Signed declaration

Name of Organisation or Individual	
Full address and contact details of Organisation (and key contact for escalation) or Individual	
Name of premises, system or Trust area for access	
Reason/Details for access to be given	
Name and Title of approving Trust Senior Manager	

As a third party, I agree that I/my organisation will abide by this Agreement and if required, I will provide evidence to assure the Trust that I/my organisation has the appropriate safeguards in place to meet the legislative requirements and Trust policies. As the Trust has an obligation to notify the ICO of a breach within 72 hours, I will immediately notify the Trust of any data breach and will fully participate in any investigation. I agree to comply with Trust policies and understand my obligations under this agreement.

Signed	
Name of signatory	
Position	
Date	
Telephone number/email (if not provided above)	

A copy of the Agreement should be retained by both the third party and the Service.