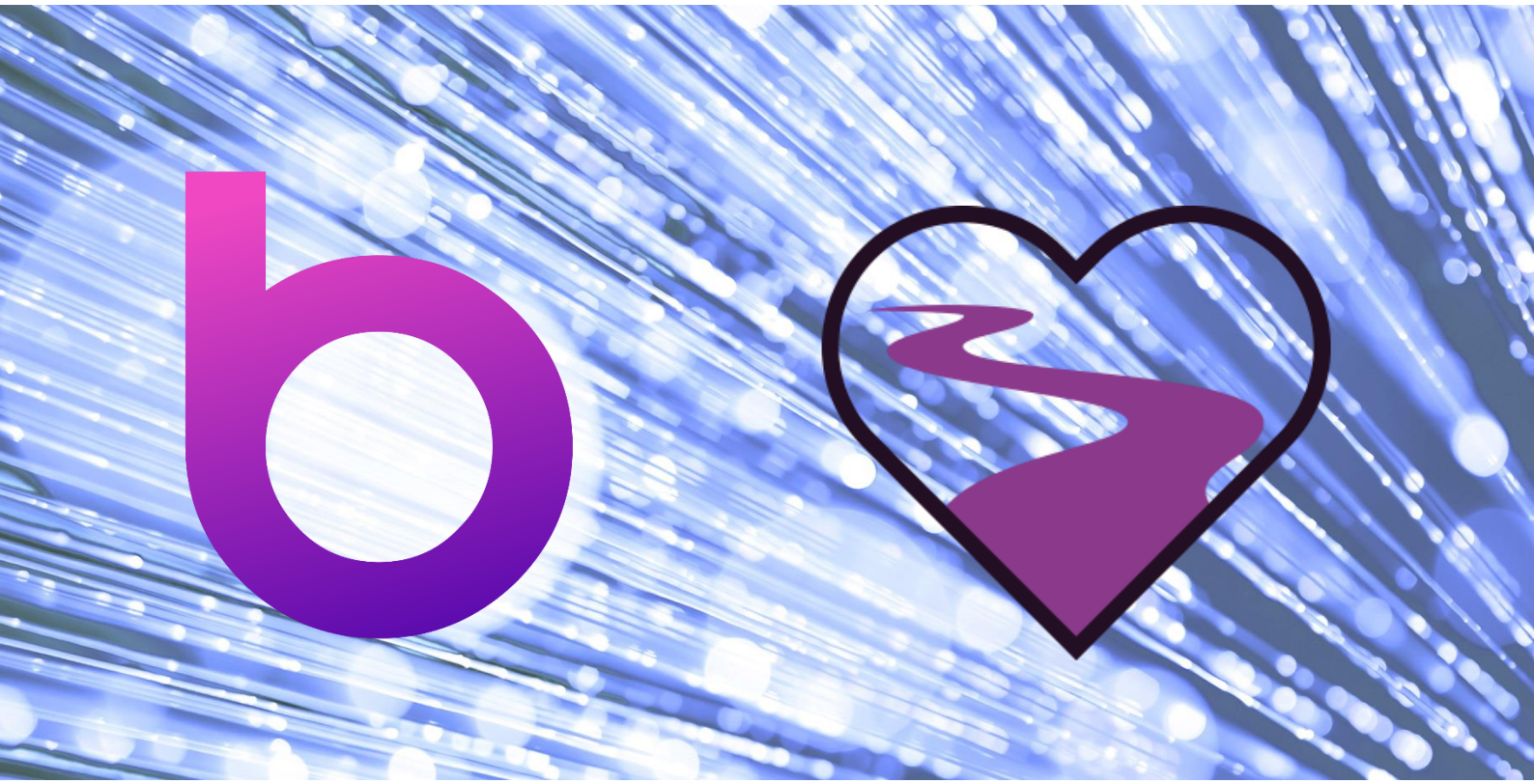
# Back-Up

## Upstream Outcomes Policy

## (Supporting Bridgit Care & Upstream health Business Units)

Author: D Crombie
Date: 04/04/2022
Version: 2.0



Information and technology
for better health and care

# Contents

# 1 Background

This policy is based on NHS Digitals example policy and aligns to the recommendations and approach adopted by NHS Digital. This is based on the NHS Digital template dated 23rd May 2017.

# 2 Approval / update history

| Version ID | Description | SIRO Approval |
|---|---|---|
| **1.0** | Initial version for release | 08/10/2018 : Darren Crombie |
| **2.0** | Updated version following 2022 review | 05/04/2022 : Darren Crombie |

# Terminology

| Term | Meaning/Application |
|---|---|
| **SHALL** | *This term is used to state a **Mandatory** requirement of this policy* |
| **SHOULD** | *This term is used to state a **Recommended** requirement of this policy* |
| **MAY** | *This term is used to state an **Optional** requirement* |

# Policy

## General

- *Upstream Outcomes **shall** schedule and perform electronic data and information back-ups in accordance with agreed Upstream Outcomes Management requirements.*
- *The frequency of back-up operations **shall** meet the needs of Upstream Outcomes to ensure a Business Continuity and Disaster Recovery Capability.*
- *On-site and remote locations where back up data is stored **shall** provide access controls and protection which reduce the risk of loss or damage to an acceptable level.*
- *Regular tests **shall** be carried out to establish the effectiveness of Upstream Outcomes backup and restore procedures by restoring data/software from backup copies and analysing the results.*
- *IT managers **shall** be provided with information relating to any issues with the backup testing of their data.*
- *Backup data/media no longer required **shall** be clearly marked and recorded for secure disposal.*

## Back-up

- *Upstream Outcomes back-up procedures and processes **shall** be fit for purpose and documented.*
- *Upstream Outcomes back-up procedures and processes **shall** be tested on implementation and at regular intervals as directed by Upstream Outcomes Management. This **should** be at least annually.*
- *All data, operating systems/domain infrastructure state data and supporting system configuration files **shall** be systematically backed up - including patches, fixes and updates which may be required in the event of system re-installation and/or configuration.*
- *Databases containing security classified or sensitive information **shall** be backed up in an encrypted format or otherwise suitably protected.*
- *Storage media used for archiving NHS data **shall** be appropriate for its expected longevity.*

- *The format in which the data is stored **shall** be carefully considered, especially where proprietary formats are involved.*

### *Restore*

- *Upstream Outcomes restore procedures and processes **shall** be fit for purpose and documented.*
- *Upstream Outcomes recovery procedures and processes **shall** be tested on implementation and at regular intervals as directed by Upstream Outcomes Management. This **should** be at least annually.*
- *Safeguards **shall** be in place to protect the integrity of data files during recovery and restoration – in particular where such files may replace more recent files.*

## 3 Key Words

***Access, Approval, Authorisation, Data, Devices, Email, Encrypted, Encryption, Information, Lock, Loss, Password, Remote, Removable Media, Secure, Security Classified, Sensitive, Systems, Theft***