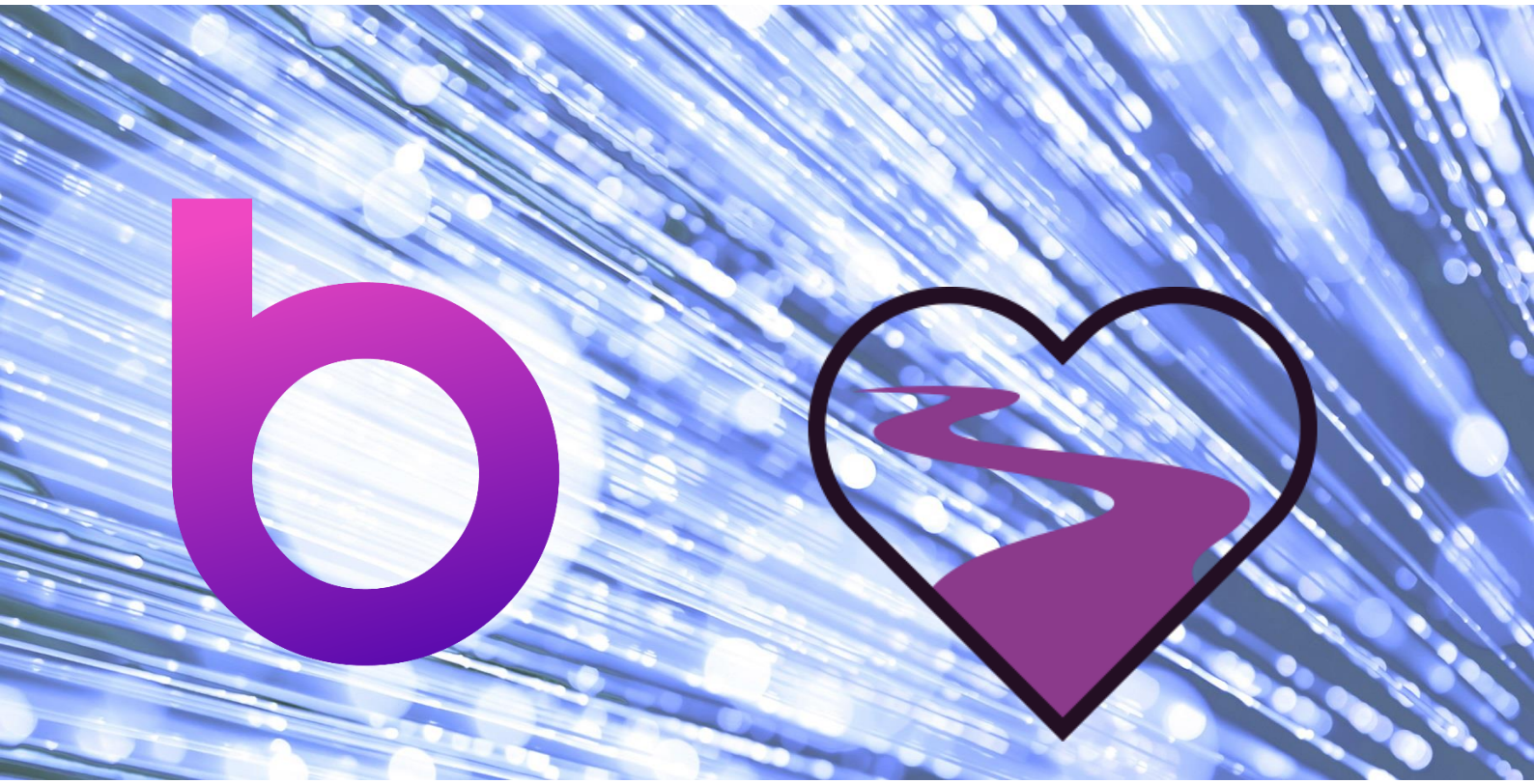
Acceptable Use

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

Use of Information Systems

Unauthorised Information Access

- *Upstream Outcomes and third party employees **shall** only be authorised access to information relevant to their work.*
- *Accessing or attempting to gain access to unauthorised information **shall** be deemed a disciplinary offence.*
- *When access to information is authorised, the individual user **shall** ensure the confidentiality and integrity of the information is upheld, and to observe adequate protection of the information according to NHS policies as well as legal and statutory requirements. This includes the protection of information against access by unauthorised persons.*

Misuse of Information Systems

- *Use of NHS information systems for malicious purposes **shall** be deemed a disciplinary offence. This includes but is not limited to:*
  - *Penetration attempts ("hacking" or "cracking") of external or internal systems.*
  - *Unauthorised electronic eavesdropping on or surveillance of internal or external network traffic.*
  - *Discriminatory (on the grounds of sex, political, religious or sexual preferences or orientation), or derogatory remarks or material on computer or communications media; this includes but is not limited to sending offending material as embedded or attached information in e-mails or other electronic communication systems.*
  - *Acquisition or proliferation of pornographic or material identified as offensive or criminal.*
  - *Deliberate copyright or intellectual property rights violations, including use of obviously copyright-violated software.*
  - *Storage or transmission of large data volumes for personal use, e.g. personal digital images, music or video files or large bulk downloads or uploads.*
- *Users accessing or attempting to access medical or confidential information concerning themselves, family, friends or any other person without a legitimate purpose and prior authorisation from senior management is strictly forbidden and **shall** be deemed a disciplinary offence.*

- *Use of NHS information systems or data contained therein for personal gain, to obtain personal advantage or for profit is not permitted and **shall** be deemed a disciplinary offence.*
- *If identified misuse is considered a criminal offence, criminal charges **shall** be filed with local police and all information regarding the criminal actions handed over to the relevant authorities.*

Guidelines for IT Equipment Use

Physical Protection

- *Users **shall** not eat or drink in the vicinity of any IT equipment.*
- *Users **shall** not expose any IT equipment to magnetic fields which may compromise or prevent normal operation.*
- *Users **shall** not expose any IT equipment to external stress, sudden impacts, excessive force or humidity.*
- *Only authorised IT support personnel **shall** be allowed to open NHS IT equipment and equipment cabinets.*
- *If left unattended in semi-controlled areas such as conference centres or customer offices, laptops **shall** be locked to a fixed point using a physical lock available from IT support.*
- *Portable equipment **shall** never be left unattended in airport lounges, hotel lobbies and similar areas as these areas are insecure.*
- *Portable equipment **shall** be physically locked down or locked away when left in the office overnight.*
- *Portable equipment **shall** never be left in parked cars, unless completely invisible from outside the vehicle and protected from extreme temperatures.*
- *Portable equipment **shall** not be checked in as hold luggage when travelling, but treated as hand or cabin luggage at all times.*

General Use

- *Users **shall** lock their terminal/workstation/laptop/mobile device (using the Ctrl-Alt-Delete function or other applicable method) when not left unattended, even for a short period.*
- *Users **shall** not install unapproved or privately owned software on NHS IT equipment.*
- *Only authorised Upstream Outcomes IT personnel **shall** be allowed to reconfigure or change system settings on the IT equipment.*
- *Laptops and mobile devices **shall**:*
  - *Only be used by the NHS or third party employee that has signed and taken personal responsibility for the laptop.*
  - *Have the corporate standard encryption software installed, rendering the information on the laptop inaccessible if the laptop is stolen or lost.*
  - *Have the corporate standard anti-virus, anti-spyware and personal firewall software installed.*
  - *Have the corporate standard remote access installed.*

- *If configured according to the specifications above the laptop/mobile device may be connected to wired or wireless access points.*
- *NHS laptops shall never be (via cable or wireless) directly connected to other non-NHS IT equipment or systems.*
- *Users **shall** not use privately owned storage devices or storage devices owned by third parties for transfers of NHS data.*
- *Any device lost or stolen **shall** be reported immediately to the Upstream Outcomes Service Team*

Internet Acceptable Use

- *Information found on the Internet is subject to minimal regulation and as such must be treated as being of questionable quality. You **should** not base any business-critical decisions on information from the Internet that has not been independently verified.*
- *Internet access via the NHS infrastructure is mainly provided for business purposes. For the purpose of simplifying everyday tasks, limited private use **may** be accepted. Such use includes access to web banking, public web services and phone web directories.*
- *Excessive personal use of the Internet during working hours **shall** not be tolerated and **may** lead to disciplinary action.*
- *Users **shall** not use Internet-based file sharing applications, unless explicitly approved and provided as a service.*
- *Users **shall** not upload and download private data (e.g. private pictures) to and from the Internet.*
- *Users **shall** not download copyrighted material such as software, text, images, music and video from the Internet.*
- *Users **shall** not use NHS systems or Internet access for personal advantages such as business financial transactions or private business activities.*
- *Users **shall** not use their Upstream Outcomes identity (i.e. using your Upstream Outcomes e-mail address) for private purposes such as on social media, discussion forums.*

NHS Email Acceptable Use

- *Email services within the NHS are provided for business purposes. Limited private use for the purpose of simplifying everyday tasks **may** be accepted but private emails **should** be distributed via web based email services.*
- *Users **shall** not use external, web-based e-mail services (e.g. hotmail.com) for business communications and purposes.*
- *Private emails **should** be stored in a separate folder named 'Private e-mail box'. If retrieval of business emails is required (due to sick leave etc.) this folder will not be subject to inspection).*
- *Private emails **should** be deleted as soon as possible in order to limit storage requirements for non-business information.*
- *Users **shall** not broadcast personal messages, advertisements or other non-business related information via NHS e-mail systems.*

- *Users **shall** not distribute content that might be considered discriminatory, offensive, derogatory, abusive, indecent, pornographic or obscene.*
- *Users **shall** not distribute statements of a political or religious nature, or other information of a personal nature.*
- *Engaging in any illegal activities via e-mail is prohibited. Discovery of such material **shall**, if deemed as being of a criminal nature, be handed over to the police.*

3 Key Words

Access, Email, Information, Internet, IT Systems, Laptop