IT Acceptable Use Policy

Document History

Document Reference:	04
Document Purpose:	This policy sets out the expectations for Bromsgrove PCN employees are required to manage information in line with legislation and national guidance.
Date Approved:	September 2023
Version Number:	1.0
Status:	Approved
Next Revision Due:	September 2024
Developed by:	Umar Sabat, Data Protection Officer
Policy Sponsor:	Chief Operating Officer
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the Bromsgrove PCN.
Associated Documents:	Data Protection Impact Assessment Policy, DSP Toolkit submission, Data Protection Policy, Privacy Policy

1. Introduction

1.1 The purpose of this document is to provide guidance to all Bromsgrove PCN employees and third parties on acceptable use of Bromsgrove PCN information and information systems.

1.2 The aim of this document is to:-

- ensure users are aware of their responsibilities in the use of Bromsgrove PCN information systems

- ensure Bromsgrove PCN's legal and statutory requirements are met

- minimise risk of inadvertent, accidental or deliverable unauthorised access or disclosure

2. Scope

2.1 This policy applies to those members of staff that directly employed by Bromsgrove PCN and for whom Bromsgrove PCN has legal responsibility, as well as any Data Processors/contractors/sub-contractors/third parties processing data or accessing Bromsgrove PCN systems. For those staff or individuals covered by a letter of authority/honorary contract or work experience, the organisation's policies are also applicable whilst undertaking duties for or on behalf of Bromsgrove PCN.

2.2 For the purposes of this policy the aforementioned will be referred to as users throughout the remainder of this document.

3. Principles and General Use

3.1 All data and information residing on Bromsgrove PCN information systems remains the property of Bromsgrove PCN at all times, unless otherwise stated.

3.2 Users accept that personal use of Bromsgrove PCN information systems is not a right and must be exercised with discretion and moderation. Users further accept Bromsgrove PCN will not accept any liability, in part or whole, for any liability for claims arising out of personal use of Bromsgrove PCN information systems or information.

3.3 Bromsgrove PCN retains the right to:

- monitor the use of its information systems for the purpose of protecting its legitimate concerns; and
- prohibit personal use of information systems without warning or consultation whether collectively, where evidence points to a risk to Bromsgrove PCN, or individually where evidence points to a breach of this or any other Bromsgrove PCN policy.

Note: Bromsgrove PCN will only monitor staff use when a legitimate need arises and with the approval of the Data Protection Officer, and only necessary information will be viewed. For further information on how Bromsgrove PCN uses data, please see the privacy policy available from our website.

3.4 Users shall adhere to Bromsgrove PCN guidelines and information NHS Mail encryption policy when sharing or sending Bromsgrove PCN information internally or externally.

3.5 Users shall not use Bromsgrove PCN information systems and information in a manner that will:

- break the law and/or have legal implications or liability to Bromsgrove PCN;

- cause damage or disruption to Bromsgrove PCN information systems;
- violate any provision set out in this or any other policy
- waste time, decrease productivity or prevent the user from performing their primary responsibilities for Bromsgrove PCN

3.6 All users shall follow Bromsgrove PCN Health and Safety guidelines when using information systems.

3.7 The below points outline general guidance that all users must adhere at all times when using IT equipment, accessing Bromsgrove PCN systems and processing data:

- Users shall lock their laptop/workstation/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 IT personnel shall be allowed to reconfigure or change system settings on the IT equipment.

4. Misuse of Information Systems

4.1 Users shall not access, attempt to access, circumvent, attempt or cause to circumvent, established security mechanisms or controls to view, modify, delete or transmit information and/or information systems to which they have not been given explicit access or authorisation.

4.2. Users shall not share their, or others, usernames or passwords to gain access to information systems, and/or information to which they have not been given explicit authorised access.

4.3. Users shall follow established procedures for password changes, and are not permitted to disclose or write down their passwords.

4.4. Users shall not install software on their Bromsgrove PCN supplied device.

4.5. Authorised staff and IT users shall not use their personal devices to connect to a Bromsgrove PCN restricted network.

4.6. Illegal download, copying and/or storage of copyrighted content onto Bromsgrove PCN information systems is strictly prohibited.

4.7 Use of NHS information systems for malicious purposes shall be deemed a disciplinary offence.

5. Physical Protection

5.1 Users shall not expose any IT equipment to magnetic fields which may compromise or prevent normal operation.

5.2 Users shall not expose any IT equipment to external stress, sudden impacts, excessive force or humidity.

5.3 Only authorised IT support personnel shall be allowed to open NHS IT equipment and equipment cabinets.

5.4 Portable equipment shall never be left unattended in airport lounges, hotel lobbies and similar areas as these areas are insecure.

5.5 Portable equipment shall be physically locked away when left in the office overnight.

5.6 Portable equipment shall never be left in parked cars, unless completely invisible from outside the vehicle and protected from extreme temperatures.

5.7 Portable equipment shall not be checked in as hold luggage when travelling, but treated as hand or cabin luggage at all times

6. Internet Acceptable Use

6.1 Usage of internet is primarily for business use. Occasional and reasonable personal use is permitted, e.g. during lunch breaks, provided that such use does not interfere with performance of duties, and does not conflict with Bromsgrove PCN policies, procedures and contracts of employment. Excessive personal use of the Internet during working hours shall not be tolerated and may lead to disciplinary action.

6.2. Users must, at all times, comply with Copyright, Design and Patent Laws, when downloading material from internet sites.

6.3. Bromsgrove PCN prohibits access to websites deemed inappropriate and monitors access and usage with the assistance of Leicestershire Health Informatics Service. The monitoring information may be used to support disciplinary action.

7. Accountability, responsibilities and training

7.1 Overall accountability for procedural documents across the organisation lies with the Chief Operating Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

7.2. Overall responsibility for the Acceptable Use policy lies with the Caldicott Guardian, who has delegated responsibility for managing the development and implementation of procedural documents to the IT service provider and line managers.

7.3. Staff will receive instruction and direction regarding the policy from a number of sources:

- Via e-mail
- Via the internet where this is stored
- When they complete IG training
- On all IT equipment provided by Bromsgrove PCN

8. Equality Impact Assessment

8 An initial Equality Impact Assessment has been carried out on this policy, and it has been deemed that there are no positive or negative impacts on any of the protected characteristics. Therefore, a full Equality Impact Assessment is not required.