5 Coles Lane, Cambridge, UK, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org
www.optimumpatientcare.org

Policy Number: POL 2400
Version Number: 5.0
Effective Date: 20 FEB 2020
Review Date: 20 FEB 2021

ACCEPTABLE IT USE POLICY

V5.0 07 FEB 2020

This is a Controlled Document. This policy is issued by the Company. Failure to comply with this policy may lead to disciplinary and/or legal action where appropriate. Human Resources Department and/or appropriate delegate should ensure the policy is communicated to all staff and contractors where applicable. The master copy of this document is kept on the Company Policies and SOPs Smartsheet and NAS drive. A copy may be made available on the Company website for public transparency. Staff may print this document for training and reference purposes but are responsible for regularly checking for more recent versions of the document.

AUTHORS	
Name:	Oliver Taylor
Position:	IT Manager / ISM
Name:	Francis Appiagyei
Position:	Clinical Manager / IG Lead
AUTHORISATION	
Name:	Chris Price
Position:	Commercial and Legal Director / SIRO Director
Signature:	
Date:	20 February 2020

CONTENT

ABBREVIATIONS

OPC or OPC UK	Optimum Patient Care Limited
POL	Policy
SOP	Standard Operating Procedure
HR	Human Resources
GP	General Practice
NHS	National Health Service
IT	Information Technology
IAO	Information Asset Owner
VPN	Virtual Private Network
IG	Information Governance
DSP	Data security and protection
DSPT	Data Security and Protection Toolkit
GDPR	EU General Data Protection Regulation 2016
DPA	Data Protection Act 2018
SIRO	Senior Information Risk Owner
ISM	Information Security Manager

BACKGROUND

Optimum Patient Care Ltd (OPC) or referred to as 'Company', supports GP practices, commissioners, health researchers and the wider NHS to improve healthcare provision to patients and better patient outcomes. This policy is important because it will help people who work for the Company to understand how to the Company's information systems and technology in an acceptable manner for work and service provision.

PURPOSE

This policy sets out the conditions for acceptable use of the Company's information systems and technology and computing services. It should be interpreted such that it has the widest application and so as to include new and developing technologies and IT services, which may not be explicitly referred to.

APPLICABILITY

This policy applies to Company staff, and associated persons such as secondees, third party and freelance contractors who use OPC IT services. Compliance with this policy is a legal and contractual duty for staff and contractors. Failure to comply with this policy may lead to disciplinary and/or legal action.

RESPONSIBILITY

All Employees and Users of OPC IT services:

- All employees and users must confirm acceptance of this policy in writing and adhere to this policy.
- Any breach of the terms of this policy or abuse of IT services is a disciplinary offence, which could result in disciplinary action, termination of employment or legal action.

Line Managers:

- Ensure this policy is adhered to in their team and that there is on-going compliance.
- Ensure any breaches of this policy are reported, investigated and acted upon via the appropriate reporting procedure.

HR Department:

- Ensure this policy is included in inductions for all employees and contractors (where appropriate).
- Ensure appropriate action is taken to address non-compliance through staff disciplinary procedures.

IT Department

- Ensure this policy is kept up to date, providing advice on request to staff on IT issues.
- Provide secure and accessible IT services which are adequate for staff working needs.
- Provide adequate training to staff and users of the Company's computing services.
- Monitoring staff compliance with this policy and support on non-compliance investigations and disciplinary procedures.

Senior Information Risk Owner (SIRO):

- Approve this policy and risk-based decisions on IT services for effective operating functions of the Company.
- Ensure appointments are in place to implement, monitor and improve IT services at the Company.

POLICY

As an employee or contractor of OPC, you have a right to use OPC's IT services. This right places responsibilities on you as a user which are outlined below.

Staff are advised of this policy during their induction and of the company's requirement for them to adhere to the conditions therein. Ignorance of this policy (or those that it directs you to), and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

For the purposes of this policy the term "**computing services**" or "**IT services**" refers to any IT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the internet and telephones).

Staff who connect their own IT or devices to the Company's network and the IT services available are particularly reminded that such use requires compliance to this policy and that usage habits may be monitored.

USER AUTHORISATION

- User ID's and passwords are not to be shared, except with IT Manager (where absolutely necessary for system administration). Users who use other user's credentials and those who share such credentials with others internally or externally will be in breach of this policy.
- Initial default passwords issued to any user must be changed immediately following notification of account set up. Passwords should be routinely changed (every 3 months is recommended) and should be changed immediately if the user believes or suspects that their account has been compromised.
- A password must only be used on one service and should not be repeated or cycled between services (a password manager can be requested to enable this).
- Users with access to significant sensitive data will be requested to change their password at least monthly or as deemed appropriate by the IT Department.

GENERAL CONDITIONS

- Your use of the Company's computing services must at all times comply with the law and the Company policies including but not limited to Information Governance Policy, Data Protection Policy, Confidentiality Policy, Data Security Policy, Records Management Policy and Business Continuity Policy.
- Your use of the Company's computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You are not entitled to use a service that you have not been authorised to use for the Company's operations.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the user's permission.
- You must not use Company computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another user or person.
- You must not use Company computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such or which promotes discrimination on the basis of race, gender, religion or belief,

disability, age or sexual orientation. (There may be certain legitimate exceptions for academic purposes which would require the fullest disclosure and special authorisations).

- You must not use the Company's computing services to disseminate mass (unsolicited) mailings or break any applicable internal or external guidelines or legislation.
- You must not install, use or distribute software for which you do not have a licence and has not been approved by the IT Department You must not use material that infringes the intellectual property rights of a third party, or that is in breach of a legal duty owed to another party.

REMOTE ACCESS

- Remote access to the Company network is possible via the Internet, Virtual Private Network (VPN) or via direct connection for specific protocols.
- Remote access from external networks or across the Internet must be made via secure methods only. If in doubt, ask the IT Department for advice. Further information and guidance is available from the Company's Information Security Policy.
- Connections via VPN or direct connections subjects the user to the same conditions, requirements and responsibilities of this policy.
- All connection attempts are logged and reportable for security and IG monitoring purposes.

MONITORING AND LOGGING

- Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time.
- Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection legislation (GDPR/DPA).
- Such records and information are sometimes required, under law, by external agencies and authorities. The Company will comply with such requests when formally submitted.

NON-ESSENTIAL USE

- All users are free to make use of Company IT equipment for personal use where such use complies with IT usage policies, is not excessive and does not interfere with Company business. This includes but is not limited to social media (Facebook, Twitter etc.), video and music streaming, forums and personal email.
- However, the Company retains the right to monitor usage and where use is overly excessive or impacts on the Company network to limit bandwidth, block usage entirely report transgressions to relevant bodies and may result in disciplinary action.

NETWORK USE

This service provides ethernet and wireless connections to Company network, plus access to services on the Internet at large.

All users have access to the following services:

- Data management provided by Google.
- Printers
- Scanners
- Network storage
- Smartsheet
- Filespace on the user's computer.

- The world wide web
- Voice over IP telephony (VOIP)

The Company reserves the right to permit or block services not specifically listed above for the purposes of security, bandwidth and traffic management, legal reasons or to protect the Company assets and its reputation.

Personal equipment connected to the Company's network must comply with certain standards (10baseT or 100baseTX) and the only protocol family supported TCP/IP. If there is any doubt, speak to IT Department for advice.

Users of the network must not run:

- DHCP servers
- DNS Servers
- Routing Protocols (such as OSPF, RIP, etc.)
- Network Discovery Protocols
- Internet Connection Sharing
- Port Scanners
- Personal servers or service hosting
    - Tor
    - Torrent seeding or downloading
    - Currency mining

Neither are they permitted to:

- Attempt DDNS dynamic Name Server Updates.
- Set up network fileshares.
- Re-distribute access to others.
- Configure any device attached with any IP address not specifically allocated to them.
- Connect any form of Wireless Access point, nor configure any computer with wireless capability such that the network can be accessed wirelessly.
- Download or distribute copyright material in breach of any licence conditions.
- Run Peer-to-Peer applications that distribute copyrighted material.

Any personal computer connected to the network service must have up-to-date antivirus and antispyware software installed at all times. Microsoft Security Essentials and SpyBot Search and Destroy are available as free downloads to users of Microsoft operating systems. All users must be running both programs at all times.

Users of any non-Microsoft based equipment should contact the IT department for advice.

There is no excuse for a personal computer connected to the network to be out of date with regards to virus, spyware or malware protection. Virus risk management is an important priority and any personal computer not adequately protected under this provision will have its access to the network disabled - until it is quarantined, inoculated and made safe.

BACKUPS

- All users of Company computer systems are required to backup all data that is not centrally stored.
- Centrally stored data includes but is not limited to email, Google Drive, NAS drive and databases.
- All other data should be backed up by the user guidance can be sought from the IT department.

DISSEMINATION & TRAINING

Dissemination: This document will be made available to staff and contractors via Smartsheet and NAS drive or on request from HR Department. This may also be in the form of a global notice sent to staff and contractors notifying them of the release of this document or made available on the Company website.

Training: Training on this document will be provided during induction of staff and contractors or as required by their training needs. Additional and/or regular training will be provided as necessary, based on training requirements to ensure continued awareness and compliance with this document.

MONITORING

Failure to comply with this policy may lead to disciplinary and/or legal action where appropriate. In the event of a breach of this Acceptable IT Use Policy the Company may in its sole discretion:
a) restrict or terminate a user's right to use the OPC IT Services;
b) withdraw or remove any material uploaded by that user in contravention of this Policy; or
c) where appropriate, disclose information to law enforcement agencies and take any legal action against a user for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

Compliance with this document will be monitored by Company senior management or appropriate delegate. This may include regular and/or ad hoc compliance checks and audits where appropriate or warranted. This document is to be reviewed annually or sooner where necessary.

RELEVANT DOCUMENTS

Information Security Policy
Information Governance Policy
Data Protection Policy
Privacy Notice
Confidentiality Policy
Document and Records Management Policy
Data Quality Policy
Business Continuity Policy
Information Incident Reporting SOP
Audits and Monitoring SOP
Staff Handbook

VERSION HISTORY

VERSION	EFFECTIVE DATE	REASON FOR CHANGE	AUTHORS
V1.0	23 JUL 2015	First final version of new policy	O. Taylor
V2.0	23 JUL 2016	Annual review and minor revisions	O. Taylor
V3.0	23 JUL 2017	Annual review and minor revisions	O. Taylor
V4.0	23 JUL 2018	Annual review and minor revisions	O. Taylor
V5.0	20 FEB 2020	New policy and new template	O. Taylor, F. Appiagyei