Ashfield

DENTAL CLINIC

Network Security Policy

Edition 1.1

Network Security Policy

Introduction

This Network Security Policy is the overarching policy for data security and protection for Ashfield Dental Ltd. (hereafter referred to as "us", "we", or "our").

Purpose

This document sets out our policy for the protection of the confidentiality, integrity and availability of the network, establishes responsibilities for network security and provides reference to documentation relevant to this policy.

Scope

This policy applies to all staff, including temporary staff and contractors. This policy also applies to our networks which are used for:

- The storage, sharing and transmission of non-clinical data and images;
- The storage, sharing and transmission of clinical data and images;
- Printing or scanning non-clinical or clinical data or images;
- The provision of internet systems for receiving, sending and storing non-clinical or clinical data or images.

Policy

Ashfield Dental Ltd.'s information network will be available when needed, can be accessed only by legitimate users, and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity, and confidentiality. To satisfy this we undertake to:

- Protect all hardware, software and information assets under its control;
- Provide effective protection that is commensurate with the risks to its network assets;
- Implement the Network Security Policy in a consistent and timely manner;
- To comply with all relevant legislation.

Risk Assessments

We will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network that are used to support those business processes.

The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity, and availability.

Physical and Environmental Security

- Critical or sensitive network equipment will be housed in secure areas, with appropriate security barriers and entry controls.
- The Information Governance Lead is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, or if they suspect the code has been compromised.
- Critical or sensitive network equipment will be protected from power supply failures.
- Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.
- Smoking, eating, and drinking is forbidden in areas housing critical or sensitive network equipment.
- The Information Governance Lead is responsible for authorising all visitors to secure network areas and for making visitors aware of network security requirements.
- All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.
- The Information Governance Lead will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.

Access Control to Secure Network Areas

- Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it.
- The Information Governance Lead will maintain and periodically review a list of those with unsupervised access.

Access Control to the Network

- Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
- Third party access to the network will be based on a formal written contract.
- All third-party access to the network must be logged.

External Network Connections

- We will ensure that all connections to external networks and systems have documented and approved System Security Policies.
- The Information Governance Lead must approve all connections to external networks and systems before they commence operation.

Maintenance Contracts

- The Information Governance Lead will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.
- All contract details will constitute part of the Information Asset register (IAR).

Data & Software Exchange

- Formal agreements for the exchange of data and software between organisations must be established and approved by the Information Governance Lead.
- All exchanges of data between organisations will be recorded on the Record of Processing Activities (ROPA).

Fault Logging

The Information Governance Lead is responsible for ensuring that a log of all faults on the network is maintained and reviewed.

User Responsibilities, Awareness and Training

We will ensure that all users of the network are provided with the necessary security guidance, awareness and training to discharge their security responsibilities.

Responsibilities

The Information Governance Lead is responsible for:

- physical security;
- updating and auditing the IAR and ROPA;
- digital access;
- managing breaches;
- data security audits.

Approval

This policy has been approved by the undersigned and will be reviewed at least annually.

Name	Christopher Renton
Signature	Christopher Renton
Approval Date	12 July 2023
Review Date	31 July 2024