Data Security and Protection Statement – Happy House Surgery

Happy House Surgery is committed to ensuring that all the personal data that it processes is done in accordance with data protection law and good data protection practice is imbedded in the culture of our staff and our organisation.

Happy House Surgery's other data protection policies and procedures include:

- record of processing activities (data mapping/data flow documentation)
- privacy notices
- personal data breach reporting process
- data retention policy (NHS Records Management Code of Practice)
- data subject rights procedure
- data protection impact assessment process
- IT security policies (NECS Acceptable User / Security Policies)

'Data Protection Law' includes the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation.
This policy applies to all personal data processed by the Practice.

Policy Framework

Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and, as part of the employment process, staff will be expected to have read, understood and signed the appropriate confidentiality document.
- Information security expectations of staff shall be included within appropriate job definitions.

Security Control of Assets

- The organisation's Corporate IT service provide a full ICT asset management process for all associated hardware and software systems (including third party systems) for the Practice
- All ICT assets, (hardware, software, application or data) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

Access Controls

- Access to information shall be restricted to users who have an authorised business need to access the information.
- Access to ICT facilities shall be restricted to authorised users who have business need to use the facilities.
- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business needs.

Equipment Security
In order to minimise loss of, or damage to, all assets, equipment are identified, registered and physically protected from threats and environmental hazards.

Protection from Malicious Software

The organisation and its Corporate ICT service providers shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Practice computers all have up to date anti-virus software. The Practice does not have access to administrative accounts: users must not attempt to install software on the organisation's property without permission from NECS and the Practice Manager.

Training

All Practice staff undertake training in IT security and protection annually.

Audit

The Practice undertakes regular audits of its procedures and systems, including the annual completion of the NHS Data Security and Protection Toolkit.

Information Commissioners Office (ICO)

The Practice is registered with ICO.