PCIG Consulting

Staff Monitoring Policy

Version: 1.0

Date: 1 April 2020

This template is for use by Practices to Comply with the GDPR requirement to have a policy regarding processing of patient data. The template is Generic in design as PCIG Consulting have clients across the UK, local sharing arrangements and area specific sharing or processing will need to be added by the practice.

Change Control

Version	To	Change	Date
1.0		New Policy	

Chapelgreen Practice

Staff Monitoring Policy

Document History

Document Reference:	…
Document Purpose:	This guidance sets out the Chapelgreen Practice guidance to staff about monitoring of work activity and the duties of confidence owed to its data.
Date Approved:	14 August 2019
Version Number:	1.0
Status:	FINAL
Next Revision Due:	April 2021
Developed by:	Paul Couldrey – IG Consultant
Policy Sponsor:	Practice Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the Practice or volunteering with the Practice.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2018
DS&P Toolkit Standard	4.3.5

Chapelgreen Practice

1. Staff Confidentiality Guidance

All your work activity on practice systems and premises is monitored in accordance with Data Protection Act 2018 and the General Data Protection Regulation 2016.

Monitoring in the workplace includes but is not limited to:

- recording on CCTV cameras
- opening mail or email
- use of automated software to check email
- checking phone logs or recording phone calls
- checking logs of websites visited
- videoing outside the workplace
- collecting information through clinical systems, to check the performance of individual staff

2. Monitoring electronic communications at work

The Practice can legally monitor phone, internet, email or fax use in the workplace if:

- the monitoring relates to the business
- the equipment being monitored is provided partly or wholly for work
- The Practice via this guidance has made all reasonable efforts to inform you that your communications will be monitored

You should bear in mind that these circumstances cover almost every situation where the Practice might want to monitor your electronic communications, the practice does not allow system to be used for personal use at all.

The Practice don't need your consent before monitoring your electronic communications for any of these reasons:

- to establish facts which are relevant to the business, to check that procedures are being followed, or to check standards - for example, listening to phone calls to assess the quality of your work
- to prevent or detect crime
- to check for unauthorised use of telecommunications systems, such as whether you are using the internet or email for personal use
- to make sure electronic systems are operating effectively - for example, to prevent computer viruses entering the system
- to check whether a communication you have received, such as an email or phone call is relevant to the business. Your employer can open your emails or listen to voicemails

3. Accessing Records of Family or Friends

Remember you are only able to access patient or staff records for business use only, this means for patients the management of their healthcare and their healthcare needs, and if you have access to staff data for employment purposes only. It is a breach of both the Data Protection legislation and common law duties of confidentiality to access any records for personal reasons. This is especially important if you work in a practice which has family members of friends as patients, you **ARE NOT** allowed (even with the persons consent) to access family members records or friends records, unless you are doing it for practice work. Obviously it would always be recommended to ask a colleague if possible to deal with family or friends when they attend or contact the practice, but in the absence of the ability to do this you must only access their record if you have a legitimate reason for doing so. Being nosey to check up on family or friends or "just looking" is a serious breach of law and your contract of employment terms which could lead to both dismissal and criminal investigation against you.

4. System Security

You are **NOT** permitted to access any practice system using another person's login details, and should never share passwords, accessing records using another person's details is a breach of Data Protection law and the Computer Misuse Act 1990, which again is a serious breach of law and your contract of employment terms which could lead to both dismissal and criminal investigation against you.

5. Basic Do's and Don't

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of NHS England.

- Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.

- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.

- Do ensure that you cannot be overheard when discussing confidential matters.

- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.

- Do share only the minimum information necessary.

- Do transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gsi.gov.uk.

- Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent and record the decision and any action taken.

- Do report any actual or suspected breaches of confidentiality.

- Don't share passwords or leave them lying around for others to see.

- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.

- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.

- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

6. Equality and Diversity

The Practice aims to design and implement Guidance documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a disadvantage over others. It considers current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the Practice must have due regard to the Public-Sector Equality Duty (PSED). This applies to all the activities for which the Practice is responsible, including Guidance development, review and implementation.

7. Due Regard

This Guidance has been reviewed in relation to having due regard to the Public-Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

8. Review and Monitoring

The Practice Manager is responsible for regular monitoring of the quality of records and documentation and managers should periodically undertake quality control checks to ensure that the standards as detailed in this Guidance are maintained.

This Guidance will be reviewed every two years unless new legislation, codes of practice or national standards are introduced.