Monitoring Policy

Audience:	All Reach South Academy Trust Employees/Workers
Approved:	May 2018
Other related policies:	Data Protection Policy Employee Privacy Notice Job Applicant Privacy Notice Data Transfer Security Policy Data Breach Notification Policy Data Subject Rights Policy Subject Access request Policy
Policy owner:	Human Resources
Policy model:	Compliance
Review:	April 2021
Version number:	1.0 April 2018

Contents

Monitoring Policy

1. Policy Statement

1.1 The Trust carries out workplace monitoring for a variety of reasons. Because monitoring includes the processing of employee data, its operation is captured by the provisions of the General Data Protection Regulation and the current Data Protection Act.

1.2 The lawful basis which applies to the Trust's monitoring processes is in order to perform the employment contract that we are party to; to carry out legally required duties and for us to carry out our legitimate interests.

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject (HMRC requirements for example and safeguarding);
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

1.3 The information and data gathered through monitoring will only be used for the purpose it was carried out for, unless the Trust identifies issues such as a breach of health and safety.

1.4 The person with overall responsibility for the operation of this policy is Andrew Mallett Only the Data Protection Officer may authorise any monitoring of employees.

1.5 As monitoring may intrude on Trust employees' private lives, monitoring will be carried out only in accordance with the General Data Protection Regulation and the current Data Protection Act. The Trust will uphold a degree of privacy at work and where monitoring is required or necessary, employees will be made aware of the extent of any monitoring together with the reasons as to why.

1.6 The Data Protection Officer will ensure the Trust is aware of its responsibilities under the General Data Protection Regulation and the current Data Protection Act. Access to the information and data collected will be secure and restricted to authorised employees.

2. Summary of Types of Monitoring

2.1 This policy supplements the Trust's policies on communications and provides for monitoring of the following types:

- crime and fraud prevention and detection;
- computer systems;
- bag searches;
- internet and email usage;
- data protection.

2.2 Monitoring of the above systems is carried out in order to fulfil the Trust's legal obligations as an employer as well as to secure their effective operation and for business reasons. Monitoring is carried out to the extent permitted or required by applicable law and as necessary and justifiable for business purposes.

3. Computer, Internet and Email Monitoring

3.1 The Trust will randomly check emails or use software to check if employees are sending, or receiving, inappropriate emails.

3.2 This monitoring ensures compliance with the Trust's policy on internet and email usage.

3.3 This monitoring may be necessary to investigate alleged misconduct, detect or prevent crime, deal with any issues surrounding the Trust's reputation, or retrieve content if an employee is absent. Performance of the system or the employee may be assessed through email and internet monitoring. Monitoring may be required to comply with legal obligations or detect/prevent crime.

3.4 Personal usage may have been permitted by a line manager or other senior colleague and monitoring will include every effort to ensure personal emails are not accessed where personal use can be clearly distinguished from business use.

4. Misconduct

4.1 Employee monitoring data may be used for disciplinary proceedings against employees.

4.2 Employees will be provided with the relevant data from the monitoring systems/processes in advance of the meeting.

5. Covert Monitoring

5.1 Covert monitoring is only deployed where the Trust believes employee(s) are carrying out a crime or other criminal activity. Covert monitoring may take place to investigate such suspicion where the Trust intends to involve the police.

6. Additional Monitoring

6.1 The Trust may, if appropriate, consult with employees in advance if it requires any additional monitoring not covered by this policy. The purpose of the additional monitoring will be identified, together with the type of monitoring necessary and any limits to achieve that purpose. There may be impacts on affected employees that the Trust will consider prior to introducing any additional monitoring. Notice will be provided to employees setting out why the Trust is introducing additional monitoring and the standards under which employees should operate.

7. Retention of Monitoring Data

7.1 All data captured as a result of employee monitoring will be kept securely. All data will be handled in a manner in accordance with data protection legal principles.