Market Sensitive Information Policy

Introduction & Objectives

1. This document sets out the principles, policies and procedures by which the FRC aims to protect *market sensitive information* (**MSI**) and guide our staff on how they should handle any information they receive or generate which they suspect may amount to MSI. The policy' objectives are:

    a. To help staff identify MSI and recognise that MSI triggers a significant publication risk (both by inadvertent leaking or planned publication);

    b. For staff to take active steps to minimise this risk by applying additional controls to the MSI as well as the FRC's standard confidentiality, information security and record keeping policies;

    c. To ensure that if the FRC deliberately releases MSI through a planned publication, we release it to the market simultaneously and in an appropriate, factual and evidence-based manner;

    d. To reduce the risk that inaccurate or sensationalist press reporting and ill-founded speculation could convert non-MSI information released by the FRC into MSI.

Principles

2. The FRC (**we**) will apply the following Principles of Good Practice:

    a. ***Policies & procedures*****:** We will maintain and operate internal policies & procedures for the use and control of MSI, which will recognise the responsibility to control access to MSI and aim to reduce the risk of its inadvertent disclosure or misuse.

    b. ***Awareness and training*****:** we will take appropriate measures, including training, to assist our staff in understanding the importance of keeping information appropriately protected and the implications of improper disclosure of MSI (including criminal and civil liability which may arise). We will aim to ensure that our policies & procedures are capable of being readily understood by all of our staff.

    c. ***Need to know and other information controls*****:** we will take reasonable steps to limit the number of staff who can access MSI received or generated by the FRC.

    d. ***Passing market sensitive information internally and externally:*** we will take reasonable care that where MSI is received or generated by staff and/or provided to a third party the staff member and the third party is aware of their obligations in relation to the use and control of the information.

    e. ***Information technology security:*** We will give appropriate consideration to the security of and access to MSI on IT systems including the implementation of controls to limit access.

Responsibility

3. The Executive Committee will be responsible for maintaining our MSI policy and internal working procedures.

4. Internal working procedures will be monitored by the Governance and Legal Team who will report at least annually to the Executive Committee.

5. Human Resources and Learning and Development will be responsible for training staff, with the assistance of the Governance and Legal Team.

6. Policies and procedures will be reviewed annually.

December 2016