COMPUTER MONITORING POLICY

1. Rationale

Grantham College monitors systems to help prevent people being drawn into terrorism and engaging in extreme views. Grantham College staff will investigate alerts from the monitoring system and take further advice where needed in dealing with possible infringements.

Impero is used as a network monitoring, management and user management application. Whilst it will not indicate that an attempt to access a particular website, or that a potentially concerning communication has been sent or received, it does log the actions of all users logged onto the College network. It will only do this, however, on a computer or laptop on which Impero has been installed. Additionally, Impero allows remote screen viewing of computers and laptops connected to the network allowing CCSS support to screen capture, communicate and take control of the remote computer.

2. Application of the policy

College staff with responsibility for monitoring the system

- Assistant Principal – Services for Students (Designated Safeguarding Lead)
- CCSS Manager
- Student Life Manager (Deputy Safeguarding Lead)
- Student Experience Manager (Deputy Safeguarding Lead)

Other members of staff, who form part of the College Safeguarding team, are also expected to support the review of and response to infringements in their role as Deputy Safeguarding Leads.

3. Topic areas deemed to be violations

The topic areas deemed to be violations areas which have been agreed for the academic year 2016-17 are listed below. These have been agreed following a review of College incidents and using information provided by Lincolnshire Police, as part of their annual Counter Terrorism Local Profile. The topic areas may change annually though for this academic year, are listed as:

- Adult Content
- Bullying & trolling
- Counter Radicalisation
- Drugs & Substance Misuse
- Eating Disorder
- Grooming
- LGBT Derogatory Language
- Race and Religious Hatred
- Self-harm
- Sexting
- Suicide
- Weapons and Violence

Searches and keywords relating to the above that are entered into any of the college systems will trigger an event that will log the details into the audit system. The system will log the following details:

- User name
- Computer used
- Date and Time
- Violation type
- Screen capture of violation

Violations that are deemed severe will be automatically emailed to the safeguarding email account that is monitored by the College Safeguarding team for them to review and respond, where required.

4. Responding to violations

a) Violations in the classroom

Lecturers have a key role in monitoring the online activity of their students whilst in classrooms and other learning environments. Through the delivery of tutorials, lessons, workshops and guest speaker talks, students should be made aware of the risks associated with cyberbullying, radicalisation and extremism. In all classrooms where computers are based, the lecturer has the ability to oversee all online activity which takes place in their classroom through Impero software.

Should lecturers witness a student accessing inappropriate online information which violates the College's Computer Use policies then they should immediately challenge the student.

Where is it felt, by the lecturer, that the violation is in relation to any of the priority areas stated within this policy, then they should contact the Designated Safeguarding Lead or one of their Deputies. The Designated Safeguarding Lead or one of their Deputies may then decide on an appropriate course of action.

Where the violation requires a response, then any actions will be noted and stored within the confidential safeguarding folder, which only the CCSS Manager, Designated Safeguarding Lead or one of their Deputies has access to.

b) Violations outside of the classroom

Not all student computer usage is supervised by College staff, specifically where students may be embarking on self-directed study or in the e-Learning Centre or Library. To respond to this, the college will monitor all computer usage through Impero software.

Where it is felt by the CCSS Manager, the Designated Safeguarding Lead or one of their Deputies, that a violation requires a formal response, then the following procedure should apply:

1. The violation is flagged by the Impero software;
2. College staff with responsibility for monitoring the system review the web pages or application which have been accessed;
3. If required, the CCSS team will produce more detailed logs of the activity from the Impero console and other monitoring systems that are in-place;

4. The CCSS team will use the Impero console to investigate alerts, each alert when selected will be marked with the name of the staff member who requested more information from the audit log;
5. College staff with responsibility make a decision to investigate the violation or decide that it does not require further investigation;
6. Where investigation is required, the staff member investigating should contact the lecturer (if the student was in a class) to enquire whether the violation came as a result of directed study/research;
7. Where the violation cannot be corroborated by the lecturer, or where a strong assumption can be made that the student (during self-directed study) may be at risk then the staff member investigating the violation should arrange an immediate interview between the student and the Designated Safeguarding Lead or one of their Deputies;
8. The Designated Safeguarding Lead or one of their Deputies may then decide on an appropriate course of action;
9. Where the violation requires a response, then any actions will be noted and stored within the confidential safeguarding folder, which only the CCSS Manager, Designated Safeguarding Lead or one of their Deputies has access to.

Quality Assurance – version control			
Review period	2 yearly	**Review carried out by**	Assistant Principal: SfS
Approved by	SLT	**Date approved**	31 January 2017
Equality Impact Assessment date	January 17	**Last review date**	January 17