GOSPORT & FAREHAM
MULTI-ACADEMY TRUST

E-Usage Policy

Next Review Date: August 2018

Policy Reviewed on: **June 2017**

SLT with Responsibility: MNS

E-Usage

The aim of this policy is to promote the safe use of the ICT by all stakeholders within the GFM.

This policy is closely related to the guidance contained in Keeping Children Safe in Education – statutory guidance to schools and colleges (DfE September 2016).

With regard to Radicalisation via the internet and social media the GFM fully adopts The Prevent Duty – departmental advice for schools and childcare providers (DfE June 2015) The policy should be read in conjunction with other relevant policies such as Engagement for Learning, anti-bullying and safeguarding policies.

Rationale

Why safe Internet use is important:

- The Internet is an essential element in 21st century life for education, business and social interaction. The GFM has a duty to provide pupils with quality Internet access as part of the curriculum and a duty of care to ensure its safe usage
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Risk Awareness

The use of e-technology can put people at risk both within and outside the GFM. Some of the dangers which may be faced include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the person.

Risk Management Statement

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to and awareness of the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks whilst using Internet facilities safely.

The GFM risk assesses to the best of its abilities and is responsible for the filtering of web content available to specific areas of learning. (See Appendix 1)

Risk Management Actions and Responsibilites

The following stakeholders all have a responsibility for ensuring that the students in the school are able to benefit from the use of ICT and know how to be safe:

Safety of the GFM Community

1. **Designated GFM employees (including DSL) are responsible for ensuring**:

- the safety (including e-safety) of members of the GFM community and will be aware of the procedures to be followed in the event of serious e-safety issues.
- that the DSL, Network Manager and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- that the day to day responsibility for e-safety issues are established, understood and reviewed
- liaison with school Network Manager
- that reports of e-safety incidents are received and creates and recorded appropriately in order to inform future e-safety developments
- regular meetings with the E-Safety Governor to discuss current issues, review incident logs and update filtering as required
- that they report regularly to Senior Leadership Team
- that confidential data is not be sent over the internet or taken off the school site unless specifically authorised.

2. **The Network Manager is responsible for ensuring:**

- Liaison with GFM excecutive to ensure that the school meets e-safety technical requirements
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
-
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

- liaison with GFM exceutive in regard to monitoring software and systems that are implemented and updated as agreed in school policies

3. **The Teaching and support staff are responsible for ensuring:**

- that they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices and that lessons include opportunities for discussing e-safety issues

- that they have read, understood and signed the school Staff Acceptable Use Policy (See Appendix 2)

- that they report any suspected misuse or problem to the designated GFM employee for investigation, action and/or sanction

- digital communications with students (email / Virtual Learning Environment (VLE)) should be on a professional level and only carried out using official school systems

- students understand and follow the school e-safety and acceptable use policy

- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- that they monitor ICT activity in lessons, extra-curricular and extended school activities

- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

4. **Students are responsible for ensuring:**

- that they use the school ICT systems in accordance with the Student Acceptable Use Policy/Home School Agreement, which they will be expected to sign before being given access to GFM systems.

- That they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- That they understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- They know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

- they understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

5. **Governors are responsible for ensuring**

- the approval of the E-USAGE Policy and for reviewing the effectiveness of the policy. This will be carried out by the full governors meetings receiving regular information about e-safety incidents and monitoring reports.

- monitoring e-safety (including incident logs) and will hold regular meetings with the designated member of the GFM

6. **Parents and Carers are responsible for ensuring**

- the endorsement of (by signature) the Student Acceptable Use Policy

- appropriate use of the school website

- that their children understand the need to use the internet / mobile devices in an appropriate way.

Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

7. **Community Users are responsible for ensuring**

- that they sign a Community User AUP before being provided with access to school systems including ICT systems / website / VLE as part of the Extended School Provision.

<u>Training withim the GFM</u>

- A planned programme of formal e-safety training will be made available to staff.

- An audit of the e-safety training needs of all staff will be carried out regularly
.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

- Governors should take part in e-safety training, with particular importance for those who are members of any sub-committee / group involved in ICT / e-safety / health and safety / child protection.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Responding to incidents of misuse

It is expected that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity, the designated GFM employee will be informed. The incident will then be reported appropriately. This could involve informing parents/carers and external authorities.

These misuses could include:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.