MOUNT ST MARY'S CATHOLIC HIGH SCHOOL

Educating the Individual for the Benefit of All

ACCEPTABLE USE POLICY

Mount St Mary's Catholic High School Acceptable Use Policy

Adopted by Mount St Marys' Governing Body on 22 January 2018

Signed  Chair of Governors

Review date: 22 January 2020

This policy should be read in conjunction with the MSM E-safety Policy, MSM Data Protection Policy, MSM Bring Your Own Device Policy, MSM Anti-bullying Policy and MSM Child Protection Policy.

Disclaimers

- In spite of the best efforts by MSM, due to the international scale and linked nature of information and the variety of languages it can be found in on the internet, it is impossible to guarantee that unsuitable material will never appear on an MSM computer terminal.
- Whilst remaining vigilant wherever possible, MSM cannot accept liability for the material accessed, or any consequences thereof:
    - The use of computer systems without permission or for purposes not agreed by MSM which could constitute a criminal offence under The computer Misuse Act 1990;
        - Methods to identify, asses and minimise risks will be reviewed; and
        - Staff, parents/carers, governors and advisers will work to establish agreement that every reasonable measure is being taken.

Need for ICT resources and usage

MSM recognises that electronic communication devices and instant internet access has long been a constant and increasing part of today's society and of the lives of society's young people in particular; they are now also an increasingly integral part of many jobs and careers, as are the skills required to use them. In order to support its students in their development, MSM continually attempts to maximise safe provision of ICT access for its students in terms of the amount and quality of resources available and time allocated to their use in lessons.

At MSM we believe that the use of ICT for learning encourages independent learning and aids directed learning, and provides access to an increasingly broad range of online readymade learning and revision resources.

MSM acknowledges that:

- ICT enables increasingly fast and effective communication and resource and information identification and sharing;
- Data and information can be easily stored and catalogued, electronic copies are far more portable than hard copies; and
- In some cases it can be appropriate, or at least acceptable, to store data and information online for ease of access, and remotely access PCs where data and information is stored, which further demonstrates the ease of access to data and information that now exists.

Security

MSM recognises that security is a very high priority consideration when creating, entering and storing data, particularly that of a personal and potentially sensitive nature. The areas of risk can be laid out broadly in five categories:

- Email
- Intranet
- All forms of data
- Individual PCs
- Internet access is provided, controlled and filtered by Schools Broadband.

Steps taken at MSM to minimise data security risks:

- Access to the MSM intranet, the internet and any in house systems contained on the MSM intranet, can only be gained by the use of an individual username and password and users are advised to have different usernames and passwords for each of their different website logins;

- All users are instructed not to share usernames and passwords with anyone and this is reinforced by regular warnings against doing so by staff;
- All users are instructed that when they leave, for any length of time, a computer terminal that they are logged onto, they should either logoff or lock the terminal to prevent unauthorised access to the MSM systems and data via their username and password;
- When using emails about school issues or business, always use the allocated school email address, never a personal one;
- Sending any sensitive (e.g. personal) data across the internet must only be done via a designated and recognised secure conduit and/or be encrypted (consult ICT Management Team for advice if unsure about what to do); and
- The most up-to-date and deemed most appropriate anti-virus and other security and protection software is installed on all computers.

Protection

1. All internet activity is monitored and logged electronically by the MSM system.
2. All internet activity leaves a permanent electronic footprint that can ultimately be traced and this includes emails and their content.
3. Software protection is installed on site and continually updated.
4. Schools Broadband control the internet provision and filtering.

These facts should always be born in mind when involved in any internet activity. Conduct and behaviour should be in line with MSM regulations, rules and guidelines as outlined in this policy and the MSM Data Protection Policy.

Websites are filtered for access. The system employed at MSM is that all websites known to be in or associated with certain categories (some of which are listed below) are blocked as a matter of course. Requests to unblock individual websites can be made, generally by staff, justified then considered by the ICT Management Team prior making a decision. It is possible that a website might be unlocked temporarily for access for the duration of a specific project or piece of work; this is more likely to occur for staff than students.

There are different levels of permission and hence access rights, which enable a level of control, and therefore protection, of students from accessing some sites inadvertently. There are automatic notification systems in place for the detection of certain words or subject matter, but staff, students and parents/carers should be aware these are not perfect.

It is worth reiterating here that the activity of each individual leaves an electronic footprint and it can therefore be monitored or checked if an individual is suspected of breaking the MSM AUP rules.

Some of the blocked website categories:

- Alcohol;
- Alternative lifestyles;
- Criminal skills;
- Extreme;
- Gambling;
- Hate speech;
- Host as an IP;
- Humour;
- Match making;
- Network timeout;
- Network unavailable;
- New URL;
- Occult;
- Phishing;
- Pornography;
- Profanity;
- Proxy anonymiser;
- Safe search;
- Search keywords;
- Sex education;
- Substance abuse;
- Weapons;
- Web chat; and
- Web email.

Roles and responsibilities

It is the Governors' role and responsibility to ensure that:

- Effective AUP and effective Data Protection Policies are written and updated regularly;
- They accept and consider all feedback about the policies; and
- The MSM Single Equality Policy and MSM Accessibility Plan are followed and employed by the Headteacher to guarantee access for all.

It is the Headteacher's role and responsibility to ensure that:

- Attention of all ICT users at MSM is drawn to the relevant policies;
- All users of ICT at MSM are aware of the monitoring of all internet activity of all users;
- Staff have the opportunity and resources to incorporate and utilise ICT in their lesson delivery;
- Prompt action is taken over any inappropriate ICT activity;
- Parents and carers are made aware of the ICT related policies and that they are available on the MSM website and in hard copy upon request (which may incur a charge to produce};
- Responsible internet use and combatting cyberbullying are included within the ICT and PHSCE curricula respectively;
- ICT facilities and resources are upgraded and tested prior to use wherever and whenever possible;
- The MSM Single Equality Policy and MSM Accessibility Plan are followed and employed by the staff; and
- The MSM website is continually developed with the inclusion of all ICT related polices among others, and curriculum areas with links to relevant sites, tips and other recommendations.

It is the Staffs' role and responsibility to ensure:

- Equality of ICT access in a classroom for all of the students therein if the ICT is to be used;
- Access rules for the internet are clearly on display where the internet is being accessed;
- Students accessing the internet are supervised at all times;
- Students are taught how to validate information obtained via the internet in the early ICT lessons following arrival at MSM;
- Problems are dealt with if and when they arise;
- They use the internet responsibly at all times in line with ICT related policies; and
- The MSM Single Equality Policy and MSM Accessibility Plan are followed and employed by the students.

It is the Students' role and responsibility to:

- Read and adhere to the MSM rules for responsible ICT use and seek explanation from staff about the rules if they fail to understand them;
- Report any material or communication that they receive or are exposed to that they consider offensive or inappropriate;
- Report loss of their username, password of known use of them by someone else;
- Refrain from giving out their personal detail to anyone other than MSM staff without strict instructions or permission from their parents/carers; and
- Follow MSM Single Equality Policy and MSM Accessibility Plan

Cyberbullying

The information below should be read as relevant guidelines for both staff and students to follow at all times.

All forms of bullying, including cyberbullying, are taken very seriously. Bullying is never tolerated and it is not acceptable for any member of staff to behave in a manner which is intimidating, threatening or in any way discriminatory. Behaviour which constitutes bullying or harassment is always taken very seriously by MSM and could result in disciplinary action which could include police involvement. This doesn't just extend to behaviour within the work place. In some instances bullying or harassment that occurs outside the workplace, where there is a link to employment, could also fall under the responsibility of the employer and therefore result in disciplinary action being taken against the responsible individual.

Certain activities relating to cyberbullying could be considered criminal offences under a range of different laws. Cyberbullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice based bullying or discrimination through a variety of media. Media used could include email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

If an allegation is received that a member of staff is responsible for comments made online which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another employee, the school will investigate this matter. Any allegation of bullying or harassment made by an employee against another member of staff where the accused uses the internet, mobile phone, text message or email, along with any other forms of abuse, could lead to disciplinary action and possibly police involvement.

Staff in schools, as well as students, may become targets of cyberbullying. Retaliation should never be resorted to i.e. personally engage with cyberbullying incidents. Incidents should be reported immediately and appropriately and support sought if needed.

Staff should report all incidents to the designated line manager or member of their school senior management team. The designated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

For various reasons, staff may find it difficult to report to their line manager in the first instance. They may want additional support or advice. They should know they can seek advice and help from their union, professional association, from Teacher Support Network, or other organisation.