The DOMINIC BARBERI Multi Academy Company

Cricket Road
Oxford
OX4 3DR
Tel: (01865) 749933
Registered in England No 084539066

Author	IT Manager	Intended target group	Principals, Business Managers, Academy Staff
Issued	November 2017	Next review due	September 2020 unless circumstances indicate amendments

AC/Nov17(04)

This policy is applicable to all DBMAC academies

e-Safety Policy

Purpose

This policy guidance aims to help everyone understand their roles and responsibilities in ensuring the safe and acceptable handling/use of information.

Roles and Responsibilities (applicable to all users of IT Systems)

Deliberate unlawful/inappropriate material must not be viewed/stored/distributed on any DBMAC owned system. This can include material which is in violation of any law/regulation or which can be considered by any reasonable person in its context to:

- be defamatory;
- be violent;
- be offensive;
- be abusive;
- be indecent or obscene;
- be discriminatory;
- incite hatred;
- constitute bullying and/or harassment; and
- breach anyone's confidence, privacy, trade secrets or copyright.

Particular care should be taken whenever you choose to use your own personal technologies in a work environment and ensure that other people, including children, are not able to see personal contents which you would deem private or sensitive. Care should be taken to keep professional and private lives separate.

Members of staff or volunteers must only make contact with students using a DBMAC provided email account or phone number. Personal email accounts, phones and social media accounts must not be used to contact students unless there are exceptional circumstances. You must inform your line manager if you have had to use your own email account, phone or social media accounts to make contact with a student for any reason.

Staff should ensure a clear professional basis for all communications with students. Staff should not give students personal telephone numbers, mobile numbers or addresses.

It is very important that staff maintain professional relationships with students at all times. This may be compromised by allowing students access to personal information e.g photographs on social media. Staff should use appropriate privacy settings on social media to ensure that students cannot access personal information.

Roles and Responsibilities

E-safety is led by an identified person within each school who has designated responsibility for it. The DBMAC Directors and Central Team will arrange for sufficient support and monitoring of eSafety within each DBMAC school.

All schools must connect to broadband via Filtered Internet Services to reduce the risk of anyone accessing illegal/unsuitable sites. This covers all users connected to the organisation's networks with the exception of the IT Services staff. Any user who accidentally accesses material they deem to be inappropriate on their own machine (or notices on another user's machine) must report this to the agreed point of reporting, which is the DBMAC IT Services Service desk: ictservicedesk@dbmac.org.uk or, if deemed sensitive, to the DBMAC IT Manager.

The DBMAC IT Manager is responsible for working alongside Principals to ensure that practices/procedures/staffing are in place that guarantee:

- all computers (and other ICT equipment) have fully up to date anti-virus protection.
- all software is properly licensed for use within school.
- appropriate measures are in place to prevent the bypassing of filtering or network security systems.
- all users have personal, identifiable and secure logons to network resources so that illegal/inappropriate use can be identified to a particular user. Shared passwords/logons should not be used.
- all users of their systems have regular updates where the latest information surrounding being e-safe can be shared.
- all users are aware of how to report suspicious activity they detect.

Staff and students should be aware that:

- all staff have the authority to confiscate and check students' personally-owned devices;
- any unacceptable usage will result in confiscation and standard school behaviour policy being applied;
- if it is suspected that the unacceptable usage could require additional investigation by school or external personnel, the device will be stored securely in school until investigations are complete.

E-Safety for Students

All students are to receive regular, age appropriate instruction to encourage safe online behaviour and responsible use of IT Systems.

IT Services across the MAC have in place various systems which are designed to monitor automatically the activity of all staff and students on MAC owned devices, with the intention of detecting safeguarding concerns. These systems may extend to live screen capture and keyword scanning for all content accessed or created.

During school, staff will guide you towards appropriate materials whilst accessing the Internet. Outside of school, you should take care regarding the use of the Internet, mobile phones and social media sites:

- You should be careful with whom you share your personal contact details. This includes email addresses and mobile phone numbers.
- You should take extra care when interacting with other people in chat rooms and online. These people may not be who they say they are.
- Do not give out personal information to people you do not know very well.
- Never agree to meet anyone who you have only had contact with online.
- To help keep you safe, share the details of the people with whom you are communicating with your parents and friends.
- Take care if accessing social networking sites such as Facebook, Twitter etc. Take care to ensure that you are using the privacy settings provided, and that you aren't revealing any information about yourself to the public.
- Do not use social media sites to post offensive material or to make yourself vulnerable to the inappropriate actions of others.

- Avoid using mobile phones and social media, in an inappropriate manner, which could be interpreted as cyber-bullying by the person receiving the communication.
- Take care - any photograph that you allow to be taken of you, or any image which you share online or via a mobile phone, can potentially be seen by a world audience via the Internet.

If you consider yourself, or another student, to be at risk, please inform an adult – either at home or school.

Prevent and Counter-Terrorism

The MAC recognises and accepts its legal responsibility to prevent young people in its care from being drawn into terrorism. All staff are trained in identifying students who may be at risk of being drawn into terrorism, and are also trained to challenge extremist ideas. Where a member of staff has a concern, this will be passed to the respective designated safeguarding leads, where action will be taken in line with our safeguarding policy.

The MAC will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools, and that suitable filtering and monitoring is in place.

Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the MAC is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain informed advice immediately.

Date Approved by Audit Committee: 15th November 2017

Verified by Company Secretary : 24th November 2017