Midsomer Norton Schools Partnership

Issued:	September 2018
Review:	Term 1 annually
LST:	MLY

ESAFETY POLICY

1 Overview

All adults within the Multi Academy Trust (known from now on as the 'Trust') must ensure that they have read and understood the implications of this policy.

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young students. Some examples of this are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

It is our duty of care alongside that of parents and other members of the community to protect our students from these dangers and this can be achieved by many different mechanisms working together. The purpose of this e-safety policy is to outline what measures the Trust takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

This E-Safety policy encompasses any electronic device that is capable of recording, storing, transferring or publishing any digital media. It includes, but is not limited to, mobile phones, laptop computers, desktop computers, tablet PC, media recorders (MP3 players) and game consoles as well as other collaboration tools and personal publishing tools. This policy highlights the need to educate students about the benefits and risks of using technology and provides safeguards and an awareness for users to enable them to control their online experience in a safe and meaningful way.

The Trust's e-safety policy should be read in conjunction with other policies including, but not limited to, AUP for ICT, Mobile Phone Policy, Student Behaviour, Bullying, Curriculum, Child Protection, Data Protection and Security and the use of Children's Images. This policy supplements all current legislation applicable to schools including the PREVENT duty as outlined in the Counter-Terrorism and Security Act 2015.

2 Teaching and Learning

2.1 Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. Each school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and pupils. Students use the Internet widely outside school on a range of devices and it is important that they learn how to evaluate Internet sources, identify potentially harmful situations and to take care of their own safety and security.

2.2 Internet use will enhance learning

The Internet access provided by the Trust has been tailored expressly for pupil and staff use and will include appropriate filtering. It is important to bear in mind that with the ever changing nature of the Internet the filtering provided by the Trust cannot be guaranteed to be 100% effective and all adults should be continually aware of the need to be vigilant when students are using technologies to access on-line materials.

Students should be taught what Internet use is acceptable and what is not and given clear objectives for Internet use when it is being used in lessons. To this end all Internet access will be planned to enrich and extend learning activities.
Staff should guide pupils in on-line activities that will support the learning outcomes planned for the Students' age and maturity.
Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation, and staff will make use of any technologies in place to monitor and restrict access to Internet resources so that its use is focused and controlled.

2.3 Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students should be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work, regardless of their age.

2.4 How will pupils learn to use ICT appropriately?

If students are to be as safe at home as they are at school, they need to recognise the risks for themselves. Each school will have a programme of teaching appropriate skills in the early years which will reinforce the safe and appropriate use of the Internet. These skills should will be revisited by staff when they use ICT to support the teaching and learning. It is the responsibility of ALL staff to ensure that any use of ICT by students is appropriate. The understanding of appropriateness will be further developed through the PSHE/learning for life curriculum and assemblies which should further develop the students understanding of the risks and opportunities of using the Internet, and social networking sites.

2.5 Staff Responsibilities

All staff are responsible for:

- Ensuring that they have an up to date awareness of e-safety matters and of the current Trust e-safety policy, practices and procedures;
- Reading and understanding the Trust's AUP;
- Reporting any suspected misuse or problem to the E-Safety Co-ordinator or Headteacher ;
- For ensuring that digital communications with students should be on a professional level and only carried out using official school systems in accordance with the Trust's ICT AUP;
- Ensuring that e-safety issues are embedded in all aspects of the curriculum and other school activities;
- Ensuring students understand and follow the e-safety and acceptable use policies;
- Helping students to gain a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Monitoring ICT activity in lessons, extra-curricular and extended school activities;
- Being aware of e-safety issues related to the use of all mobile devices and that they monitor their use and implement current school policies with regard to the use of these devices;
- Ensuring that where internet use is pre-planned its use is guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- Ensuring that where sound and video media that is based on streaming services, its use is pre-planned and that the whole material has been checked as being suitable for the age of the students that are accessing the material.

2.6 Cloud Storage

Employees to the Trust must note that:

- Not all cloud based storage technologies are safe and secure. The Trust follows the guidance provided by the DFES and at the time of review, the only recognised cloud storage permissible by the staff in the Trust are Google Drive and Microsoft One drive.
- Staff should not store any other data related to their day-to-day work in any other cloud based systems without first discussing this with the Director of ICT.

3 Managing Internet Access

3.1 Information system security

- The capacity and security of the ICT systems provided by the Trust will be reviewed regularly;
- Virus protection will be automatically updated regularly;
- Where computers have access to sensitive financial data over the Internet, additional security software will be installed to protect the finances of the Trust.

3.2 E-mail

- All emails sent from the ICT systems within the Trust to external bodies will encompass a standard footer statement
- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation by pupils should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Where necessary a Whole-class or group e-mail addresses should be used at Key Stage 2,1 and below;
- Access in school to external personal e-mail accounts may be blocked. This is because it will not be secure and conform to the relevant legislation governing security of data.

3.3 Published content and the school Website

- The contact details on the individual school Web sites will be the school address, e-mail and telephone number.
- Staff or students' personal information will not be published.
- The designated Web Site Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing pupil's images and work

- Photographs that include students will be selected carefully and will not enable individual students to be identified. These will be vetted by a member of the leadership team;
- Student's full names will not be used anywhere on any Web site or Blog, particularly in association with photographs;
- Each school will record on the MIS system all parents who object to their children's pictures being used in publicity;
- Written permission from parents or carers will be obtained before photographs of students are published on any website;
- Student work can only be published with the permission of the student.

3.5 Social networking and personal publishing

- Only authorised members of staff will be granted access to social media sites with the remit of publicising the individual schools. Access by all other staff will be blocked or filtered by the Trust's filtering systems.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students and parents will be advised that the use of social network spaces outside school can be dangerous
- Staff will be advised not to have social network sites, but where they do they must be secure, and must not have any 'friend' that is a current of ex-student.
- Staff must not under any circumstances communicate with any student through social networking sites.

3.6 Managing filtering

- The Trust will ensure that the systems in place to protect pupils are reviewed and improved on an annual basis;
- The Trust will proactively add inappropriate websites to the filter lists as appropriate. Unblocking may only be permitted once the site has been discussed with the e-Safety coordinator;
- If staff or students discover an unsuitable site, it must be reported to a member of the ICT support teams who will then refer it to the e-Safety Coordinator. In certain circumstances they may filter the site immediately until a review of the site can be undertaken;
- ICT Support staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- Any material that the school believes is illegal will be reported to the Headteacher in the first instance. Should it be necessary, this will then be passed to the relevant authorities.

3.7 Managing video conferencing

- Any IP videoconferencing use must be discussed with the Director of ICT before its use.
- Any IP videoconferencing must be to a recognized and verified end destination
- Students will not be allowed unsupervised access to Videoconferencing facilities

3.8 Managing emerging technologies

- Technologies are continually changing and emerging. Whilst it is not possible to cover all such devices, it is intended that the policies of the Trust have been written in such a way that they cover most new technologies;
- There is a separate Mobile Phone Policy which addresses their use within the school environment. This policy also covers the use of mobile phones whilst on any trip organized by the school;
- Students need to be aware that the sending of abusive or inappropriate text messages is forbidden and will be dealt with under the guidance of the individual schools Behaviour Policy;
- Staff will be issued with a school mobile phone where contact with pupils is required for example on foreign trips or outward bound activities. Staff should not issue their personal phone numbers to students;
- The use of portable media devices including for example the iTouch is acceptable so long as use is appropriate. Wireless access points have been provided by the Trust in each school to encourage the students to use them to support their studies. The Internet access afforded through these devices is via the normal filtered Internet Access.

3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Any misuse of data must be reported to the safety coordinator immediately;
- Staff will ensure that they lock the terminal should they need to be away from their desk to prevent unauthorised access to student data;

- Student data can only be uploaded to recognised safe and secure cloud storage as defined by Her Majesty's Government. Currently the only two ratified safe and secure cloud storage are: Microsoft One Drive and Google Education accounts. Personal Google accounts are NOT secure under the terms of the Data Protection Act 1998.
- Student data taken home must be protected by suitable means;
- Some schools in the Trust will be able to share student data via the Web. Where this is the case it will only be shared with parents/guardians with a priority setting of 1 or 2. All accounts will be secured by username and password;
- The school will undertake appropriate backups to protect the personal data on the computer network.

4 Policy Decisions

4.1 Authorising Internet and email access

- All users of the system must read and sign the 'Acceptable Use Policy' before using any ICT resource. Parents will be asked to counter sign and return the student AUP form. (Some schools may have the form in the front of the student planner. It is suggested that a paper copy is also kept on the student's record in the pastoral office).
- Upon leaving the school the accounts for both Staff and students will be disabled for a period before being deleted.

4.2 Assessing risks

- The Trust will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer within the Trust.
- The Trust will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

4.4 Community use of the Internet

- The Trust will liaise with local organisations to establish a common approach to e-safety. Special accounts may be set up specifically for community use;
- The Trust may not afford access to the Internet by any external contractors for any reason as it breaches security and firewall procedures.

5 Communications Policy

5.1 Introducing the e-safety policy to pupils

- The AUP will be frequently displayed on all user's screens before they are permitted to logon to the system. Users must agree to the terms otherwise the system will automatically log them off the system.
- Students will be informed that network and Internet use will be monitored and should be reminded by staff when undertaking Internet based research projects.
- Staff will remind students when ICT is used to support learning in any classroom;

5.2 Staff and the e-safety policy

- All staff will be given the School e-Safety Policy;
- Staff will be made aware that Internet access is monitored and traced to the individual user. Discretion and professional conduct is essential.

5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively, and parents will be advised accordingly.

6 e-Safety Violations

6.1 Handling e-safety complaints

- Complaints of Internet or email misuse by students will be investigated and supervised by the eSafety Coordinator/ Head of Pastoral care who will in conjunction with pastoral staff implement any relevant punishment, which could include bans for either Internet or email or both. Letters will be sent to parent/guardians outlining the offence and the sanctions imposed. A record of this misuse will be logged on the School's MIS system;
- Complaints of Internet or email misuse by staff will be referred to the head teacher;
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

6.2 Abuse of mobile devices and media within school

- The schools within the Trust will take a serious and robust approach to any misuse of technology which occurs on any site. If the abuse is via a mobile phone, the phone will immediately be confiscated and an investigation undertaken by the Head of Pastoral care;
- Parents/guardians will be informed about the incident and any resulting actions taken as punishment;
- Where necessary, external agencies will be informed including the Police;
- All such incidents will be logged on the individual school's MIS system.

6.3 Abuse of mobile devices and media outside of school

- Although rare, it is an increasing occurrence where modern technology is used to cause offence and hurt outside of the school. Where the school becomes aware of the issue they will take a serious and robust approach to the misuse;
- Parents/guardians will be informed about the incident and any resulting actions taken as punishment;
- Where necessary, external agencies will be informed including the Police;
- All such incidents will be logged on the individual school's MIS system.

7 Bring Your Own Device (BYOD):

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the Trust encouraging students to bring their own technologies into the school environment, especially at Post 16, in order to provide a greater freedom of choice and usability. There are, however, a number of e-safety considerations for BYOD. The Trust is clear that the use of BYOD should not introduce vulnerabilities into existing secure environments. For this reason, the Trust will extend any policy relating to the use of technologies to any device that is provided by the Trust or that is classed as a BYOD.

The Trust has a set of clear expectations and responsibilities for all users:

- All users adhere to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible these devices will be covered by the Trust's normal filtering systems, while being used on the premises.
- All users will use their username and password to access the ICT systems and Internet via a BYOD;
- Students are reminded that misuse of their own equipment is covered by the Trust's policy as if it were a misuse of the Trust's equipment.

8 Scope of the Policy

This policy applies to everyone within the Trust (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of the ICT facilities provided by the Trust, both in and out of the School buildings.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. The Trust will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.