MATTHEW MOSS
HIGH SCHOOL
Learning for Life

Policy No.: 30

Policy: Internet and E-Safety

Review Date: June 2017

Policy Name: Internet and E-Safety

Nominated Lead Member of Staff: E-Safety Co-Ordinator

Review Cycle: 1 Year

Authorisation: Headteacher

Review Date: June 2017

INTERNET AND E-SAFETY POLICY

SYNOPSIS

This policy sets out a definition of the school's internet and e-Safety Policy. It should be read in conjunction with the appropriate Acceptable Use Policy (Staff or Learner). It defines appropriate use and restrictions of the use of the school's IT systems.

Introduction

e-Safety Policy

e-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's internet Policy has been revised and refocused to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-Safety policy will operate in conjunction with other policies including those for Learner Behaviour, Bullying, Curriculum, Data Protection and Security.

The Matthew Moss High School Core Policy

This core e-Safety policy provides essential basic coverage. It contains all the elements we consider are mandatory in order to protect staff, learners, and the school.

1.1 End to End e-Safety

e-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and learners; encouraged by education and made explicit through published policies.
- Sound implementation of e-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure internet access including the effective management of content filtering.

Naturally policy must be translated into practice to protect learners and educate them in responsible ICT use.

1.2 Teaching and Learning

1.2.1 Why internet and ICT use is important

- The internet and ICT are essential elements of 21st century life for education, business and social interaction. The school has a duty to provide learners with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and learners.
- It is used to significantly contribute to raising educational standards, promote learner achievement, support the professional work of staff and to enhance the school's management functions within a safe and responsible environment

1.2.2 How internet use enhances learning

- The school's internet access will be designed expressly for learner and staff use and will include filtering appropriate to the age of learners.
- Learners will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Learners will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

1.2.3 Learners will be taught how to evaluate internet content

- The School will ensure where possible that the use of internet derived materials by staff and by learners complies with copyright law.
- Learners will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Learners will be taught to acknowledge the source of information used and to respect copyright.

1.3 Managing Internet Access

1.3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly by the ICT Manager and ICT Technicians in collaboration with SLT.
- Virus protection will be installed and updated regularly.
- Security strategies will be monitored for appropriateness and effectiveness.
- Personal data sent over the internet will be encrypted or otherwise secured.
- Unapproved software will not be allowed to be stored anywhere on the network or attached to email. Files held on the school's network will be regularly checked

1.3.2 Email

- Personal email or messaging between staff and learners is not permitted
- Learners and staff may only use official school-provided email accounts on the school system and to communicate with each other.
- Learners must immediately tell a teacher if they receive offensive email.
- Staff must immediately tell a member of SLT if they receive offensive email.
- Learners must not reveal personal details of themselves or others in email communication and must never arrange to meet anyone.
- Email sent to parents or an external organisation may only be sent using an official school-provided email account and should be written carefully and with consideration, in the same way as a letter written on school headed paper.
- Access in school to external personal email accounts may be blocked

1.3.3 Published content and the school Website

- The contact details on the Website will be the school address, email and telephone number. The personal information of learners will not be published.
- The Business Manager, as nominated by the Headteacher, will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing learner's images and work

- Photographs that include learners will be selected carefully and will not enable individual learners to be identified.
- Learners' full names will not be used anywhere on the Website without parental permission, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of learners are published on the school Website even where names are not given.
- Work may only be published with the permission of the learner and their parent or carer.

1.3.5 Social networking and personal publishing

- The school will block/filter access to social networking and newsgroups unless a specific educational use is approved.
- Learners will be advised never to give out personal details of any kind which may identify them or their location.
- Learners will be advised not place personal photos on any social network space.
- Learners will be advised on security and advised to set passwords, deny access to unknown individuals and how to block unwanted communications. Learners should be encouraged to invite known friends only and deny access to others.
- Staff wishing to use Social Media tools with learners as part of the curriculum will risk assess the sites before use and check the site terms and conditions to ensure the site is age appropriate.
- Access to forums and chat rooms that are moderated by a responsible person or organisation and are directly linked to an educational activity will be permitted subject to risk assessment.
- Staff must not run social network sites for learner use on a personal basis.

- Official school social networking sites, such as a twitter feed, will be operated by a limited number of staff. The Digital Resources Co-Ordinator will have overall editorial control.

1.3.6 Managing filtering

- The school will work in partnership with Rochdale LEA and the DfE to ensure systems to protect learners are reviewed and improved.
- If staff or learners discover an unsuitable site, the URL must be reported to the e-Safety Coordinator or the IT Technicians.
- SLT 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 must be reported to appropriate agencies such as the Police, the IWF or CEOP.
- Changes to the school filtering policy will be risk assessed by staff with technical and educational experience prior to any changes and, where appropriate, with consent from SLT.

1.3.7 Managing the Cloud Environment

- SLT and staff will regularly monitor the usage of the cloud by learners and staff in all areas.
- Learners/staff will be advised about acceptable conduct and use when using the cloud.
- Only members of the current learner, parent/carers and staff community will have access to the cloud.
- All users will be mindful of copyright issues and will only upload appropriate content onto the cloud.
- Any concerns with content may be recorded and dealt with in the following ways: a) The user will be asked to remove any material deemed to be inappropriate or offensive. b) The material will be removed by the site administrator if the user does not comply. c) Access to the cloud for the user may be suspended. d) The user will need to discuss the issues with a member of SLT before reinstatement. e) A learner’s parent/carer may be informed
- When staff, learners, etc. leave the school their account or rights to specific school areas will be disabled.

1.3.8 Managing mobile phones and portable devices

- The use of mobile phones and other personal devices by learners and staff in school will be decided by the school and covered in the school Acceptable Use or Mobile Phone Policies.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by a member of SLT with or without the consent of the learner or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence, it will be handed over to the police for further investigation.
- Mobile phones will not be used during lessons or formal school time unless the member of staff, or group of learners, have notified the relevant staff and educational value is clear.
- Electronic devices of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.
- If a learner breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Learners found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the learner’s withdrawal from either that examination or all examinations.
- Learners should protect their phone numbers by only giving them to trusted friends and family members. Learners will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Members of staff are advised that personal mobile phones and devices must be switched off or switched to ‘silent’ mode, Bluetooth communication should be “hidden” or switched off and mobile phones or devices will not be used during

teaching periods unless permission has been given by a member of SLT in emergency circumstances.

- If a member of staff breaches the school policy then disciplinary action may be taken.

1.3.9 Managing video and audio technology

- Care should be taken when capturing photographs or videos that all learners are appropriately dressed.
- Staff may use photographic or video devices, including digital cameras and mobile phones, to support school trips and curriculum activities.
- Learners will always seek permission from their teacher before making audio or video recordings, taking photographs or making or accepting a videoconference call.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential. Non school sites must checked that they are delivering material appropriate to the learners involved.
- When recording a videoconferencing session, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of the videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing will be appropriately supervised for the learners' age.
- Videoconference contact information will not be put on the school website.

1.3.10 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Learners will be instructed in the safe and appropriate use of personal devices both on and off the school site.

1.3.11 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Our Data Controller is Michelle Johnston

- All staff will ensure that they lock their screen or log off before leaving any computer screen unattended to minimise Data Protection risk and must understand that failure to do so may result in disciplinary action being taken.

1.4 Policy Decisions

1.4.1 Authorising internet access

- All staff must accept the terms of the ‘Responsible Internet Use’ statement before using any internet resource in school.
- The school will maintain a current record of all staff and learners who are granted access to school ICT systems.
- Learners will only obtain access to the internet by agreeing to abide by the Responsible Internet Use Statement in their planner. Parents are asked to countersign this, giving permission for their child to access the internet at school.

1.4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that access to unsuitable material will never occur via school device. Neither the school nor Rochdale LEA can accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The use of computer systems without permission or for inappropriate purposes may constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the police.

1.4.3 Behaviour

- Cyberbullying, along with all other forms of bullying, of any member of the school community will not be tolerated. Full details are set out in the school’s anti-bullying and behaviour policies.
- The sending of abusive or inappropriate text messages is against the law and appropriate measures will be taken against perpetrators.
- When publishing materials, learners and staff will consider the thoughts and feelings of those who might view it. They are advised not to publish specific

detailed or private thoughts, especially those that may be considered threatening, upsetting or defamatory.

- Inappropriate material will not be downloaded onto school hardware.
- Breaching this e-Safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.

1.4.4 Handling incidents of concern

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and in any other relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or Rochdale LEA e-Safety officer and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the Rochdale LEA e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other schools in Rochdale.

1.4.5 How will e-safety complaints be handled?

- Complaints of internet misuse will be dealt with under the School's Complaints Procedure.

- Any complaint about staff misuse will be referred to the SLT.
- Learners and parents will be informed of the complaints procedure.
- Parents and learners will need to work in partnership with the school to resolve issues.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

1.4.6 Community use of the internet

- The school will be sensitive to internet related issues experienced by learners out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for learners whilst using the internet and technology on the school site

1.5 Communications Policy

1.5.1 Introducing the e-Safety policy to learners

- e-Safety rules and/or copies of the learner Responsible Use Policy will be posted on the school website.
- Learners will be informed that network and internet use will be monitored and can be traced to the individual user.
- Learners will only obtain access to the internet by agreeing to abide by the Responsible Internet Use statement in their planner.

- Safe and responsible use of the internet and technology will be reinforced across the curriculum and subject areas and reminders regarding safe and responsible use given prior to internet access.
- A module on responsible internet may be included in the form time programme.
- Particular attention to e-Safety education will be given where learners are considered to be vulnerable.

1.5.2 Staff and the e-Safety policy

- All new staff will be inducted in the key parts of this policy as part of their induction.
- All staff including teachers, learning support assistants and support staff will be provided with the School e-Safety Policy and have its importance explained.
- All staff must ensure that data is kept secure, confidential and accurately communicated.
- Staff should be aware that network and internet use can be monitored and traced to the individual user; discretion and professional conduct is essential.
- Up to date and appropriate staff development in safe and responsible internet use, both personally and professionally, and on the school internet policy will be provided as required
- Staff that manage filtering systems or monitor ICT use will be supervised by SLT and have clear procedures for reporting issues.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

1.5.3 Enlisting parents’ support

- Parents must give permission for learners to have internet access by signing the Responsible Internet Use Statement in their son’s homework diary.
- Parents’ attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Website.
- All parents are invited to a talk in Year 7 regarding e-Safety.

- Interested parents will be referred to relevant organisations.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home internet use, or highlighting e–Safety at other attended events e.g. parent evenings.

1.6 Responsibilities

1.6.1 SLT

- One member of SLT will have specific responsibility for the implementation of this policy.
- Members of SLT will monitor the quality of ICT use and its impact on behaviour, attainment and quality of teaching.
- The data lead on SLT must ensure that data is kept secure, confidential and accurately communicated.

1.6.2 Headteacher

- The Headteacher must ensure that this policy is monitored and regularly reviewed

1.6.3 Governors

- The Governors must evaluate this policy for effectiveness in meeting its objectives
- The Governor responsible for Safeguarding will include e-Safety in their regular report to the Local Governing Body.

1.6.4 Heads of Faculty

- HOFs must model the practice outlined in this policy and inform learners and the staff that they line manage of their responsibilities.
- HOFs must ensure consistent application of the policy by members of their department.
- HOFs must ensure that subject-relevant material is up to date on both the school website and cloud.

1.6.5 Teaching Staff

- All staff must model the practice outlined in the policy, inform learners of their responsibilities and monitor and reinforce appropriate usage.
- All staff will ensure that they lock their screen or log off before leaving any computer screen unattended to minimise Data Protection risk and must understand that failure to do so may result in disciplinary action being taken.
- All staff must ensure the safe use of ICT and care of ICT equipment in their classrooms.
- All staff will ensure that instruction in responsible and safe use for learners precedes internet access.

1.6.6 In General

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for learners. The school will take all possible precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is difficult to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Rochdale LEA can accept liability for the material accessed, or any consequences of internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- Breaching this e-Safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.

1.7 Writing and reviewing the e-Safety policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

- The school has appointed an e-Safety coordinator who is Tony Salter
- Our e-Safety Policy has been written by the school. It has been agreed by SLT and approved by governors.
- The governor responsible for Safeguarding is also responsible for e-Safety and will include e-Safety in their report to the Local Governing Body.

Associated Policies:
All areas of School Policy