E-Safety Policy

This policy should be read in conjunction with:

- Data Protection Policy (GDPR)
- Safeguarding Policy
- Anti-Bullying Policy
- Peer-on-Peer Abuse Policy

Introduction

At William Morris Sixth Form (WMSF) we are committed to providing a safe and secure environment for student, staff and visitors and promoting a climate where young people and adults will feel confident about sharing any concerns which they may have as a result of online safety issues. It highlights the need to educate 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.

Covid-19 Addendum

WMSF recognises the increased risk when students are learning remotely. Monitoring of students' online behaviour is much more difficult and students will be going online more often and for more time than when face-to-face learning occurs. We have written home to parents to advise them on potential risks associated with online learning, and offered training on the WMSF website. We also continue to make online safety a focus in tutorials and in online lessons.

Scope

WMSF recognises that risks posed online are considerable and multi-faceted, and can change quickly. It is important that all staff are aware of this and keep up to date with any emerging online risks. Nonetheless, WMSF policy to keep young people safe can be broadly defined by three categories:

1) **Contact**: the potential the internet and other technology allows for malicious or dangerous contact with other individuals or groups.
2) **Content**: the potential for exposure to offensive, illegal and inappropriate material.
3) **Conduct**: the potential for inappropriate conduct online.

Roles and Responsibilies

The following section outlines the e-safety roles and responsibilities of individuals and groups within the School:

- **Leadership Group**: to promote Internet Safety across the school and ensure staff are trained on these issues as part of their induction.
- **Assistant Principal (Behaviour)**: to monitor behaviour and handle any cases of cyber-bullying or inappropriate conduct online.
- **Designated Safeguarding Lead (DSL)**: to follow up on any cases where students' safety is at risk online, or where students are engaging in potentially risky behaviour.
- **Senior Tutors**: to embed Internet Safety resources as part of the PSHE curriculum in their cohorts so that tutors are prepared and trained to deliver activities and information.
- **Technical Services**: to implement LGFL filters, monitor internet use and report immediately to the DSL/LG any concerns they find about students' use of the internet, monitor staff internet use.
- **All staff**: to adopt safe internet use standards (see Staff Code of Conduct) and discuss what these are with students, to take responsibility for their professional development on e-safety.

The E-Safety Officers are:

Anthony Evans: Designated Safeguarding Lead (DSL)
Shiraz Hasham: Learning Technologies Manager

The E-Safety Officer is responsible for:

- dealing with e-safety incidents in their joint capacity as E-Safety Officer and Designated Safeguarding Lead (DSL) in accordance with the School's Safeguarding Policy;
- taking day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the School's e-safety policies and documents;
- ensure that staff are aware of the procedure that needs to be followed in the event of an e-safety incident;
- liaise with Technical Services to ensure that security systems in place are operational and effective from a technical perspective e.g. filtering systems
- maintaining and regularly reviewing an E-Safety procedure to identify potential patterns of behaviour, to determine if any changes to this policy are required and to inform future e-safety developments.

Technical Services:

The Learning Technologies Manager is responsible for ensuring that:

- the School's technical infrastructure is secure and is not open to misuse or malicious attack;
- the School meets required e-safety technical requirements as specified in the Acceptable Use Policy which is available on K:\Admin\Personnel\Policies and Procedures
- users may only access the networks and devices in accordance with the School's Acceptable Use Policy.
- the filtering policy is applied and updated on a regular basis in accordance with this policy.
- investigations into any e-safety incident in accordance with this policy are reported to the E-Safety Officer;
- they keep 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;
- the use of the School's network and devices is logged, and records can be provided and searched on request to ensure compliance with all the Acceptable Use Policies in order that any misuse / attempted misuse can be reported to the E-Safety Officer for investigation;
- the School's antivirus system definitions and web filter categories are updated automatically.

Guidelines

WMSF recognises that the internet and digital communications are an important part of everyday life and we do not believe that banning its use within school will protect students from the harm it may potentially cause. However, there are many measures WMSF can take to ensure its students are kept as safe as possible when using online technology.

Why the Internet and digital communications are important

- The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

Internet use will enhance and extend learning

- Staff will be made aware of and students will be educated in the safe use of the internet.
- Clear boundaries will be set and discussed with staff and students, for the appropriate use of the Internet and digital communications.

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

- Esure that the use of Internet derived materials by staff and by students 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.

Managing Internet Access

- The school has a secure fibre-optic broadband connection to the Internet through the London Grid for Learning (LGFL) and connects to the private National Education Network.
- The LGFL Web Filtering system blocks sites that fall into categories such as pornography, racehate, gambling and sites of an illegal nature.
- The school ICT system security is reviewed regularly.
- Virus protection will be installed and updated regularly.

Managing E-mail

- Students and staff should only use approved WMSF e-mail accounts (user@wmsf.ac.uk and user@wmsf.me.uk).
- Students must be made aware of how they can report abuse and who they should report it to.
- Students must report any offensive or inappropriate e-mail they receive to a member of staff.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- Staff must use the school E-mail account for communicating electronically regarding school business.
- The use of WMSF E-Mail is solely for professional use.
- Staff must follow additional steps to ensure sensitive data is secure when sending information via E-mail.

Published content and the school web site

- Staff or student personal contact information will not generally be published.

- The Assistant Principal (Engagement) will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Published students' images and work

- Photographs that include students will be selected carefully so that images of individual students cannot be misused.
- Students' full names will not be used anywhere on the Trust Web sites or other on-line space, particularly in association with photographs.
- Written permission will be obtained before photographs of students are published on the school website.

Social networking and personal publishing

Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Students must be made aware of how they can report abuse and who they should report abuse to.
- Students should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.
- Staff are advised not to run social network spaces for student use on a personal basis.
- Staff will be advised not to include work related contacts (parents, pupils or ex-pupils) on their social network space.
- The discussion of work related matters/information by staff, on a social network site is forbidden and would become a disciplinary matter.
- Staff must be aware that information stored, displayed or discussed on social networking sites are in the public domain.
- Parents, students and staff should be aware that bullying can take place through social networking sites.

Managing monitoring and filtering

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or students discover an unsuitable site, it must be reported to a member of staff or the Technical Services department.

- Logs of internet breeches are kept and reviewed. Access to any illegal, suspicious websites will be reported to the appropriate agencies.

Managing videoconferencing

- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for students by Teaching staff.
- Staff will establish dialogue with other conference participants to make an assessment of the risk, before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material suitable for the curricilum.

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.
- The sending of abusive or inappropriate text messages is forbidden.
- The use by students of cameras in mobile phones will be kept under review.
- The use of mobile phones during lessons or formal school time is forbidden.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation (GDPR).

- Data that contains sensitive information, be it personal information or work related information (eg documents about pupils) needs to be encrypted to ensure its safety. This applies whether data is on a hard drive or portable storage device.
- Users must securely delete personal or sensitive data when it is no longer required.
- Any personal or financial data transferred electronically should be encrypted or password protected.

Policy Decisions
Authorising Internet access

- The Technical Services department will maintain a current record of all staff and students who are granted access to school ICT systems.

Assessing risks
Handling e-safety complaints

- Complaints of Internet misuse will be reported to the Schools Technical Services Department and the E-Safety Officer.
- All School staff have a duty to report any online activity by a colleague which raises concern. Staff should refer to Safeguarding Policy for further guidance. This is particularly important where the welfare of students may be at risk.

The school's Technical Services department will take all reasonable precautions to prevent access to inappropriate 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 connected to the school's network. The Technical Services department cannot accept liability for any material accessed, or any consequences of Internet access.

The Technical Services department will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective. The Technical Services department will ensure monitoring software and appropriate procedures are in place.