Mougins School
E-safety Policy

Author:	Head of Pastoral Care/DSL/HM/Head Of Primary	Date:	September 2020
Reviewed/authorised:	SLT	Date:	October 2020

Contents

1 Introduction

The Mougins school e-safety policy aims to create an environment where students, staff, parents, governors and the wider school community work together to inform each other of ways to use the Internet responsibly, safely and positively.

Through teaching ICT we equip children and young people to participate in a rapidly-changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyse, exchange and present information in a varied and stimulating way. ICT skills are a major factor in enabling them to be confident, creative and independent learners. As the aims of ICT are to equip children and young people with the skills necessary to use technology to become independent learners, the teaching style that we adopt is as active and practical as possible. We provide suitable learning opportunities for all children and young people by matching the challenge of the task to the ability and experience of the child.

Internet technology helps students learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour when achieving this. students, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour. These agreements and their implementation will promote positive behaviour which can transfer directly into each student's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a list of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer Internet usage and year on year improvement and measurable impact on e-safety. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

2 The Mougins School E-Safety Policy Scope

The school e-safety Policy and agreements apply to all students, staff, support staff, external contractors and members of the wider school community who use, have access to or maintain school and school related Internet, computer systems and mobile technologies internally and externally. The school will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and Internet usage both on and off the school site. 'In Loco Parentis' provision under the Children Act 1989 also allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of students.

The e-safety policy covers the use of:

- School based ICT systems and equipment
- School based intranet and networking
- School related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing.
- School ICT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets
- student and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or Internet facilities
- Tablets, mobile phones, devices and laptops when used on the school site.

3 Managing Information Systems

When securely maintaining information it is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and learners.

- Local Area Network (LAN) security issues include:
- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use, as detailed in the Mougins School ICT Acceptable Use Policy.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date. Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with WPA2 PSK (pre-shared key).

Wide Area Network (WAN) security issues include:

- Mougins School broadband firewalls are configured to prevent unauthorised access between schools.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used unless it has been encrypted and virus checked.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the network will be regularly checked.
- System capacity in relation to storage will be checked regularly.
- The use of user logins and passwords to access the network will be enforced.

4 Filter Management

The school's broadband access provides filtering appropriate to the age and maturity of learners. There is flexibility in the filtering system to allow for changes in provision depending on the learning required.

Any breaches in filtering should be reported to: n.wright@mougins-school.com

If staff or learners discover unsuitable sites, the URL will be reported to Nigel Wright who will then record the incident and escalate the concern as appropriate.

The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.

Any material that the school believes is illegal will be reported to appropriate agencies.

The school`s access strategy will be designed by educators to suit the age and curriculum requirements of the learners, with advice from network managers.

5 Monitoring the E-safety policy:

The e-safety policy will be actively monitored and evaluated by an e-safety committee. This committee will comprise:

- E-safety Coordinator/Officer (Nigel Wright)
- Head Teacher (Simon Hollands)
- Designated Safeguarding Lead (Robert Cooke)
- Head of Primary School (Christine Bearman)

6 E-safety policy review and evaluation schedule

The E-safety policy and Acceptable Use Policy are reviewed at or prior to the start of each academic year. Additionally, the policy will be reviewed promptly upon:

Serious and/or frequent breaches of the acceptable Internet use policy or other in the light of e-safety incidents.

7 Responsibility for e-safety

7.1 The Board of Proprietors' responsibility for e-safety:

The Head Teacher will liaise directly with the Board of Proprietors with regard to reports on e-safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community.

7.2 ICT support staff and external contractors

External ICT support staff and technicians are responsible for maintaining the school's networking, ICT infrastructure and hardware. They are aware of current thinking and trends in ICT security and ensure that the school system, particularly file-sharing and access to the Internet is secure. They further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking. Our ICT Manager (n.wright@mougins-school.com) maintains and enforces the school's password policy.

7.3 Teaching and support staff

Teaching and teaching support staff need to ensure that they are aware of the current school e-safety policy, practices and associated procedures for reporting e-safety incidents.

Teaching and teaching support staff will be provided with e-safety induction as part of the overall staff induction procedures.

All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the ICT Acceptable Use Agreement

All staff need to follow the school's Staff Code of Conduct, in regard to external off site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on internet school messaging or communication platforms, for example email, VLE messages and forums and the school website.

All teaching staff need to monitor student internet and computer usage in line with the policy during school time. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site.

Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.

Teaching staff should be aware of online propaganda and help students with critical evaluation of online materials.

Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

7.4 E-safety in the Mougins School curriculum

'Teaching online safety in school (DfE, June 2019) outlines to schools the importance of helping children and young people not only use the internet safely, but also give them opportunities to learn how to behave online. Throughout the new compulsory Relationships (Sex Education) and Health Education students will be taught what positive, healthy and respectful online relationships look like.

The PSHE curriculum will be following the underpinning knowledge and behaviours:

- How to evaluate what they see online
- how to recognise techniques used for persuasion;
- online behaviour;
- how to identify online risk;
- how and when to seek support.

Throughout the curriculum teaching about potential harms will include:

- Age restrictions
- Content
- Disinformation, misinformation and hoax
- Fake websites and scam emails
- Fraud (online)
- Password phishing
- Personal data
- Persuasive design which keeps 'users online for longer than they might have planned or desired'
- Privacy settings
- Targeting of online content
- Abuse (online)
- Content which incites hate, violence
- Fake profiles

- Grooming
- Live streaming
- Pornography
- Unsafe communication
- Impact on confidence (including body confidence)
- Impact on quality of life, physical and mental health and relationships
- Online vs. offline behaviours
- Reputational damage
- Suicide, self-harm and eating disorders

E-safety is accessed as part of pastoral care, in, for example:

- Form time activities,
- assemblies,
- year group presentations,
- tutorial opportunities.
- E-safety events – such as Safer Internet Day and Anti Bullying Week.

7.5 Designated Safeguarding Lead

The Designated Safeguarding Officer is trained in specific e-safety issues. Accredited training with reference to child protection issues has been accessed.

The Designated Safeguarding Officer can differentiate which e-safety incidents are required to be; reported to CEOP, Gendarme, ASE, Parquet de Grasse, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.

Possible scenarios might include: allegations against members of staff; computer crime – for example hacking of school systems; allegations or evidence of 'grooming'; allegations or evidence of cyber bullying in the form of threats of violence, harassment or malicious communication; producing and sharing of Youth Produced Sexual Imagery (YPSI).

7.6 Students

Are required to use school Internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies. students are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.

Students need to be aware of how to report e-safety incidents in school, and how to use external reporting facilities, such as the ASE 119 number.

Students need to be aware that school Acceptable Use Policies cover all computer, Internet and mobile technology usage in school, including the use of personal items such as phones. students need to be aware that their Internet use out of school on social networking sites such as Instagram is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and students in terms of cyber bullying, reputation, or illegal activities.

7.6 Parents and Guardians

It is hoped that parents and guardians will support the school's stance on promoting good Internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.

The school expects parents and guardians to sign the school's Acceptable Use Agreement, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as extranets, websites, forums, social media, online reporting arrangement and questionnaires.

The school will provide opportunities to educate parents with regard to e-safety through the school website.

8 General Data Protection and e-safety:

The GDPR sets out the key principles that all personal data must be processed in line with.

Data must be: processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected

There are also stronger rights for individuals regarding their own data.

The individual's rights include: to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all.

The General Data Protection Act is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

8.1 Use of IT facilities for curriculum teaching and learning:

Use of the Internet and IT facilities should be clearly planned prior to the activity. Websites and software Apps should be suggested, Students should be trusted to be responsible when researching the Internet, and teaching staff will consider the age and maturity of the students.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: students, parents, staff and external agencies. Personal and sensitive information should only be sent by e-mail when on a secure network.

Personal data should only be stored on secure devices. In other words, only computers, servers, file- servers, cloud space, or devices which require a user name and password to access the information.

Secure accounts need to be logged off after use to prevent unauthorised access.

Personal emails should not be used for school business

9 E-safety - UK and France

This e safety policy takes cognizance of the following UK legislation: The Education and Inspections Act 2006 (Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of students off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the school behaviour policy.) Computer Misuse Act 1990, sections 1-3 Data Protection Act 1998 General Data Protection Regulations Freedom of Information Act 2000 Communications Act 2003 section 1,2 Protection from Harassment Act 1997 Regulation of Investigatory Powers Act 2000 Copyright, Designs and Patents Act 1988 Racial and Religious Hatred Act 2006 ; Protection of Children Act 1978 Sexual Offences Act 2003

Schools have a 'duty of care' to students and as such act "in loco parentis." Under the UK's Children Act 1989, this enables schools to remove personal information, cyber bullying and comments relating to school students as if they were the child's parent.

At Mougins School, the Head Master reserves the right to examine the contents of a student's mobile device if there is a suspicion of cyber-bullying, or unacceptable use.

10 Useful links and numbers

- CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
- Childline: www.childline.org.uk
- Childnet: www.childnet.com
- Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk
- Cybermentors: www.cybermentors.org.uk
- Digizen: www.digizen.org.uk
- EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact local Police.
- Kidsmart: www.kidsmart.org.uk
- Think U Know website: www.thinkuknow.co.uk
- Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

In France

- A.S.E. Aide Sociale à L'Enfance 04 97 18 60 00
- National Number for Children 119
- Cellule d'Urgence des Mineurs 04 92 60 72 19
- French Ministry of Justice *cybeharcèlemenr* site: https://www.service-public.fr/particuliers/vosdroits/F32239#:~:text=Le%20harc%C3%A8lement%20via%20internet%20
- *Non au harcèlement* site: https://www.nonauharcelement.education.gouv.fr/que-faire/faire-face-au-cyberharcelement/