Moor Park
HIGH SCHOOL • SIXTH FORM
Excellence in All

Digital Safeguarding Policy

Approved by SLT : 5 November 2019

Contents

1. Changes

- Amendment to 8.1 to add in the GDPR legislation.

2. Statement of Intent

This policy is intended to ensure pupils at Moor Park High School and Sixth Form are protected while using digital technologies at the school.

The school is committed to including digital technologies, in particular internet use, in our curriculum. In doing so, we recognise the inherent risks posed by these useful learning tools. Full compliance with this policy will mitigate these risks and help to ensure pupils are safe online.

3. Introduction

3.1. While digital technology and the internet provide an exciting opportunity for pupils to learn and interact with various subjects, they also pose a risk, with the potential for exposure to inappropriate content and inappropriate contact from other children and adults. Digital technology also provides an opportunity for pupils to engage in unacceptable behaviour, both online and offline.

3.2. In order to keep pupils safe online, and for them to learn how to keep themselves safe online, all pupils and teachers should be aware of relevant skills and strategies needed to ensure internet safety. This ranges from knowing to only use the internet with adult supervision for younger pupils, to strategies for identifying appropriate links for older children.

3.3. Mitigating the risk to pupils created by digital technology and the internet will be ensured through specific safety lessons and will also be embedded within the general curriculum.

3.4. E-safety will depend on policies being properly implemented at all levels of the school community: from published policies, to a secure school network design, the effective management of school broadband and filtering systems, parental awareness of the dangers of online use and effective teaching about digital-technology use.

3.5. This policy is to work in conjunction with our Safeguarding Policy, Cyber Bullying Policy, Mobile Phone Policy and Social Media Policy.

4. Aims

4.1. At Moor Park High School and Sixth Form we are committed to using the internet and other digital technologies to:

- Make learning more exciting and interactive.
- Make lessons more varied.
- Enable pupils to gain access to a wide variety of knowledge in a safe way.
- Raise educational standards.
- Prepare our pupils for using the internet safely outside of school and throughout their education.

5. Definition

5.1. Digital safety encompasses a number of technologies such as computers, tablets, collaboration tools, internet technologies, mobile devices and more.

6. E-Safety Measures

6.1. The school's internet system, and access to it, is specifically designed for staff and pupil use and, as such, includes filtering appropriate for secondary age children.

6.2. Pupils will have clear objectives about why they are using the internet whenever the internet is incorporated into lessons.

6.3. Lessons using the internet will be carefully planned and the 'access levels' classes and pupils are afforded will be fully considered, taking into account pupil age and curriculum requirements.

6.4. Children using the internet will do so in classrooms (or other appropriate shared areas of the school) during lesson time only and with teacher supervision.

6.5. Pupils will be taught what internet use is acceptable and unacceptable, and teachers should be vigilant during internet based lessons.

6.6. Particular vigilance is necessary if and when pupils are undertaking internet searching. Teachers should use their professional judgement regarding whether this internet function is appropriate for the relevant class.

6.7. If the Google images website is used in class, this should be done using the 'safe search' function. Teachers can make judgement calls on whether to allow the use of Google images at all, due to the range of content and possibility for accessing inappropriate material.

6.8. Records will be maintained detailing all staff and pupils who have internet access.

7. School Policies

7.1. Information system security:

- Moor Park High School and Sixth Form uses Virtue Technologies to provide broadband with the appropriate firewall and all appropriate filters.
- The security of the information systems and ICT system capacity will be reviewed regularly.
- The virus protection will be regularly updated. There should be procedures in place for virus protection to be updated on any laptops used by staff members or students.

7.2. Email and digital communications:

- Only approved school e-mail accounts may be used at school/via the school network. Additionally, pupils must not receive or access personal e-mail accounts.
- Pupils should notify a teacher immediately if they receive an offensive e-mail.
- Pupils should be taught about the dangers involved in e-mail communications. They should be taught:
- Not to reveal personal details about themselves or others in e-mail or digital communication. This will generally include full names, addresses, mobile or landline phone numbers, school name, instant messenger (IM) address, e-mail address, names of friends, specific interests and clubs etc.
- Never to arrange to meet someone they have 'met' via e-mail/online without appropriate safeguarding measures (e.g. the presence of a parent or responsible adult).
- That online communications are 'real' and as such require the same respect for others as face-to-face interactions.
- Parents and pupils alike should both be informed of the risks inherent in using social media. Social media websites will not be accessible through the school's network and should not be accessed on school devices through other networks except where agreed with the Senior Leadership Team. A log of allowed social media websites will be kept with the ICT Support Team.
- The school's ICT Support Team will maintain a list of 'inappropriate' and 'banned' terms. The use of these in e-mails will be detected and logged.

7.3. The school website:

- The Schools Website Team has overall responsibility for the content of the school website. This includes ensuring all content is appropriate and accurate. There are procedures in place for authorising the uploading of any content onto the school's website.
- No personal information or contact details will be published on the school's website. This extends to the use of pupil's full names. The school address, e-mail and main telephone number should be the only contact information available to website visitors. Where agreed, other contact information may be made available.

- The uploading of any images or photographs of pupils onto the school website requires parental permission in writing which is obtained at the beginning of the year through the Photography and Videos School Policy. Any images should be carefully chosen with safeguarding in mind and it is advisable that pupils are not easily identifiable in images. Pupil's full names should never be used in conjunction with their photograph on the website.

7.4. Managing filtering:

- The ICT department will work with the web filtering supplier to ensure filtering systems are appropriate, efficient and as effective as possible. This will entail regular checks and ongoing monitoring.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the ICT Support Team. There are processes in place to deal with such reports.
- Protecting personal data:
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

7.5. Complaints:

- Complaints regarding pupil misuse of the school's internet/digital devices will be dealt with by the network manager and an appropriate, senior member of staff. Sanctions for misuse may include:
  - Revocation of internet use privileges
  - Communication with the pupil's parents/carers
  - Detention or other usual discipline methods
  - Staff misuse of the internet or digital technology should be referred to the headteacher.
- Any issues or complaints of a child protection nature should be dealt with according to the school's Child Protection and Safeguarding Policy procedure.
- Information on the complaints procedure should be published on the school's website and parents should be informed about this.

7.6. Digital technology/internet use outside of school:

- Parents should be informed of the inherent risks of internet use.
- The school will be aware of, and responsive to, any issues pupils experience via their use of the internet or digital technology outside of school. The school's Cyber Bullying Policy may also be relevant in such instances.

8. Monitoring

8.1. The law related to internet use is changing rapidly and staff and pupils need to be aware of this. Relevant laws include:

- The Computer Misuse Act 1990
- The Public Order Act 1986
- The Communications Act 2003
- The Sexual Offences Act 2003
- The Malicious Communications Act 1988

- The Copyright, Design and Patents Act 1988
- The Protection of Children Act 1978
- The Obscene Publications Act 1959 and 1964
- The Protection from Harassment Act 1997
- The EU General Data Protection Regulation 2018

8.2. This policy should be monitored and updated to account for changes in the legal landscape, such as amendments to the outlined laws. The ICT Systems Manager is responsible for updating this policy and ensuring the school remains in compliance with its legal obligations.