MORE HOUSE SCHOOL

POLICY

E-SAFETY - CYBER BULLYING, MOBILE PHONES, & USE OF ICT

Rationale:

The internet holds huge potential for young people. It is a fun and exciting place to explore and it helps children and young people to learn at home as well as in school. The internet and use of mobile devices are now a part of the daily social and educational lives of children and young people, and it is therefore vitally important that we are aware of the risks so that children can make the most of the opportunities available to them while remaining safe.

- Cyber bullying is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Keeping Children Safe in Education 2020 (KCSIE 2020 updated January 2021) recognises bullying as a form of peer-on-peer abuse. Cyber bullying is any form of bullying that involves the use of mobile devices, internet or other forms of digital media. Examples include, sending offensive text or voice messages and emails, circulating offensive images on the internet, or impersonating someone on social networking sites such as Facebook, Instagram and Snapchat. The potential for online social media to be used for the purposes of grooming a child for sexual exploitation is also well recognised.

More House School is committed to developing a safe environment where the students act respectfully and positively towards each other in acceptable and non-threatening ways. More House School provides its own information-technology system incorporating hardware, and e-mail and internet access. All staff and students are required to sign a user-agreement before use.

Purposes:

- To teach pupils how to stay safe in the digital environment and how to manage their own behaviour to avoid making themselves vulnerable to a range of risks, including online grooming and sexual exploitation (see Relationships and Sex Education Policy).
- To ensure staff, parents and pupils fully understand the risks that derive from this technology.
- To enable staff, parents and pupils to learn how to avoid exposing themselves to such risks.

Broad Guidelines:

- With technology being an integral part of the lives of all our pupils, we recognise that blocking and barring sites is no longer adequate. We need to teach all of our pupils to understand why they need to behave responsibly if they are to protect themselves. Our technical staff play a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of our hardware system, our data and for training our teaching and administrative staff in the use of I.C.T. The use of the school internet, email, programmes and software, by any member of the School community, is monitored by various technologies including Smoothwall Monitor, which provides immediate reports of any inappropriate or concerning usage to the Designated Safeguarding Lead and key support staff.
- We will not tolerate any illegal material and will always report illegal activity to the police, Local Safeguarding Children Partnership (LSCP) and/or any other appropriate agency. If we discover that a child or young person is at risk as a consequence of online activity, we

may seek assistance from CEOP (Child Exploitation and Online Protection command). We will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy and anti-bullying strategy.

- Our anti-bullying policy and strategy describe our preventative measures and the procedures that will be followed when we discover cases of bullying. Proper supervision of pupils plays an important part in creating a safe I.C.T. environment at school, but everyone needs to learn how to stay safe outside of the school. We value all of our pupils equally. It is therefore part of the ethos of More House School to promote considerate behaviour and to value diversity both offline and online. The school is committed to promoting amongst its entire community respect for, and accordance with the fundamental British Values of democracy, the rule of law, individual liberty and mutual respect for and tolerance of those with different faiths and beliefs, and those without faith. Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he/she should not be afraid to come forward.

Staff at the school have the responsibility to ensure that:

- they adhere to the Code of Conduct for all adults within the school;
- all forms of cyber bullying are prohibited, and the staff is aware of cyber bullying and is able to identity and look for signs of occurrence among the students;
- students are aware of the consequences of cyber bullying, online grooming and the viewing of inappropriate material;
- students adhere to the acceptable use policy for technology, including computers and mobile telephones, whilst on school premises;
- their personal technology, not provided by the school, must not be used to film or record any image of pupils, either on or off the school site;
- all concerns relating to suspected cyber bullying, online grooming or the viewing of inappropriate material must be reported to a member of staff and responded to promptly;
- there is supervision of technology that is effective for monitoring and deterring cyber bullying, online grooming and the viewing of inappropriate material;
- They report any concern through the appropriate channels;
- any internet links sent to pupils for them to engage in independent learning will have been vetted prior to sending.

Students at the school have a responsibility to ensure that they:

- adhere to the Acceptable Use of IT policy for pupils;
- do not participate in cyber bullying in any form, or the viewing of inappropriate material;
- do not use any mobile phones, cameras or other digital devices to record audio and visual material that is not authorised as part of the school curriculum;
- do not breach the privacy of students, staff and members of the school community through any unauthorised recording or filming;

- do not disseminate inappropriate material through digital media or other means;
- report incidents of suspected cyber bullying, online grooming or the viewing of inappropriate material to a member of staff, or use the school misuse desktop reporting system;
- advise students being victimised by cyber bullying, or concerned about inappropriate on-line or computer activity, to talk to an adult;
- offer to speak to an adult on behalf of the student who is being victimised by cyber bullying.

Keeping the School Network Safe

- Certain sites are blocked by our filtering system and our systems are monitored by designated staff with the aid of Smoothwall Monitor, in order to identify and prevent any radicalisation and extremism that might exist, along with any inappropriate or concerning usage.
- Designated staff monitor the Smoothwall Monitor alerts, and the I.T department block SPAM and certain attachments. Social chat and networking sites, such as Facebook, are blocked globally by the web-filtering system, so as to protect students from risks including, but not limited to grooming, bullying and online sexual exploitation. Restricted access is facilitated at agreed times after normal school hours, where there is a higher level of supervision by the staff. Internet usage is monitored and filtered by both category and age of user. Older pupils are granted more freedom than younger pupils with their internet usage, but are still monitored in the same way. Residential pupils are granted different access levels outside of school hours to enable them to have more freedom in their boarding homes.
- We issue all pupils with their own personal school email address. Access is via a personal LOGIN, which is password protected. We give guidance on the reasons for always logging off and for keeping all passwords secure.
- We have strong anti-virus protection on our network, which is operated by the I.T. Department.
- The School's wireless network affords pupils and adults access to the Internet using their own devices through a Bring Your Own Device (BYOD) system, which is subject to the same filtering system as the school's computers. Monitoring of users' activity is more difficult, and the school's management deliberately provides such access in areas that are public, so that members of the staff may supervise pupils' use. The wireless access in the residential accommodation is closely monitored by the residential staff who seek to be a prominent presence in all areas of the boarding houses during residential hours. The wireless access is disabled overnight.
- Pupils and adults in the school may find they are able to access the Internet using 3G, 4G and 5G connections on their personal hand-held devices. Such access to the Internet is again difficult to monitor, but arrangements for permitting the use of such devices encourage such access to occur in public areas with a high level of staff supervision, and in the residential

accommodation for boarders where there is again close supervision by members of the residential staff.

- Pupils experience frequent learning opportunities relating to appropriate use of technology and the internet, including lessons delivered by the School's staff as part of the PSHEE and RSE curriculum. Pupils are encouraged and taught how to report misuse or concerns.
- School staff regularly use online video-sharing platforms (such as, but not limited to, YouTube) to enhance learning and support the curriculum. On occasions, staff may, include specific videos for pupils to view as part of their independent learning. In such circumstances, staff will scrutinize all videos for suitability of content and audience prior to distribution. Parents give their consent for their son to receive such links at the time of admission.
- The school recognises that there is usually a minimum age to use such platforms (YouTube's Terms of Service (March 2020) state that, "You may use the Service if you are at least 13 years old."). Parents are requested to give their consent to allow their son to receive video-sharing links as part of his independent studies.
- Although More House School recognises the value of the extensive educational content available on video-sharing services, the school has no control over third-party content and advises parents to ensure that suitable restrictive controls and supervision are in place. It is also advisable to disable the 'autoplay' function, which automatically plays another video based on the user's viewing history.

Consideration When Using Mobile Phones/Electronic Equipment

- Mobile phones, iPods and other personal electronic devices should be switched off and stored securely during the school day. They may be used during breaks, lunch times and at the end of the school day, after afternoon registration. Teachers are free to decide whether appropriate use of mobile phones is needed within their own lessons.
- Staff may confiscate personal equipment that is being used inappropriately during the school day and during boarding time.
- Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

Other sources of information

- The School newsletter provides regular updates in the 'Safe at School' article. This regularly communicates advice or notices about how parents can protect their children in relation to e-Safety, and activities in school.
- The School website has a Safeguarding and e-Safety page with useful links and information for parents supporting the development of their understanding of risks and protective measures.

- The School is a member of National Online Safety, and regularly posts updates on e-safety, including parent guides to many different apps and sites, on the school website and social media platforms.

Conclusion:

We expect pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face to face contact. Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated.

- Useful online resources are available from the following sites:
  - Childnet International (www.childnet-int.org)
  - Vodafone Digital Parenting (www.vodafone.com/content/parents.html)
  - Digizen (www.digizen.org.uk)
  - Cyber Mentors (www.cybermentors.org.uk)
  - Cyberbullying (www.cyberbullying.org)
  - E-Victims (www.e-victims.org)
  - Bullying UK (www.cbullying.co.uk)
  - CEOP/Thinkuknow (www.iwf.org.ukthinkyouknow.co.uk)
  - Internet Watch Foundation (www.iwf.org.uk)
  - Advice for parents and carers on cyber bullying DfE 2014
  - Cyber bullying: advice for head teachers and school staff DfE 2014

Appendix A - The following School policies and documents form important continuations of this policy:

- Acceptable Use (I.T. users) Agreement
- Age-Regulated Audio and Visual Digital Media, Including Independent Access to the Internet policy
- Anti-Bullying Policy
- Anti-Bullying Strategy
- Safeguarding, incorporating Child Protection policy
- Parental Permission Form for the Use of Equipment Enabling Independent Access to the Internet, Including Mobile Telephones (permission form)
- Preventing Radicalisation and Extremism Policy
- Relationships and Sex Education policy
- Keeping Children Safe in Education 2020 (KCSIE)
- Working together to Safeguard Children (2018)