Kingsmeadow
Inspiring minds

Online Safety Policy
Updated October 2020

To be updated October 2021 LTh

EQUALITIES STATEMENT

Kingsmeadow School is committed to equal opportunities for all and the policy will be applied equally to all members of the school community regardless of age; disability; gender reassignment; pregnancy and maternity; race; religion or belief; sex and sexual orientation.

We are committed to providing a calm, caring and well-ordered environment where everyone feels safe, happy and understands the expectations of attitudes to learning in order to create an ethos conducive to excellent learning and teaching for all.

We promote a culture of praise and encouragement and expect consistency of response to both positive and negative behaviour.

We believe that positive relationships based on mutual respect, promote positive attitudes to learning and that as students learn by example, all adults within the school should act as positive role models with regard to their own behaviour.

Equality Targets

Everyone at Kingsmeadow School must strive to accept and meet the differing needs and aspirations of all members of the school community, using human resources and skills available to us all to:-

1. Safeguard individuals from all forms of abuse and harassment. We must ensure that victims can be confident of support and, where appropriate redress. We must ensure that aggressors can never claim the excuse of acting out of ignorance.

Success Criteria

- Incidents of aggression and bullying are rare and dealt with effectively and outcome of which are recorded on our MIS (Management Information System).

2. Establish a school ethos built on mutual trust and respect. We should treat others as we would wish to be treated. We should respect other people, their property and school premises.

Success Criteria

- Students regularly receive merits and praise for their positive attitudes to learning, respect to others, their school campus and their local community.
- Incidents of disrespectful behaviour are rare and dealt with promptly and effectively and the outcome of which are recorded on our MIS..

3. Safeguard the rights and freedoms of others. We must actively pursue our aim to help students develop personal moral values which respect the values and tolerates differing religious and cultures.

Success Criteria

- Racist and homophobic incidents are extremely rare and dealt with promptly and effectively and the outcome of which are recorded on our MIS.
- Students display tolerance, support of and celebrate other cultures/religions through their work.

4. Develop an organisation which maximises pupil opportunity and experience. We must ensure that the curriculum and other activities encourages and supports the opportunity for all. We must ensure that students are not excluded from activities because of status or income.

Success Criteria

- All student groups are able to access the curriculum fully and discreet intervention results in specific gaps in student achievement narrowing and in line with the whole school population

and national figures. E.g. boys, girls, students with SEND and students receiving free school meals.

Online Safety Policy

Internet technology helps students learn creatively and effectively. It encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The Online Safety policy encourages appropriate and safe conduct and behaviour during this process.

Students, staff and all other users of school-related technologies are expected to follow the guidelines set out in this policy and promote positive behaviour at Kingsmeadow.

Online Safety Policy scope:

This policy applies to all students, staff, external contractors and members of the wider school community who use, have access to, or maintain school and school-related internet and computer systems internally and externally.

The Online Safety Policy covers the use of:

- School-based ICT systems and equipment
- School-based intranet and networking
- School-related external internet including, but not limited to, extranet, online learning platforms, blogs, social media websites
- External access to internal school networking such as webmail, network access, file-serving (document folders) and printing
- Student and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or internet facilities

Reviewing and evaluating Online Safety and ensuring good practice:

This policy should be read in conjunction with the school Data Protection Policy, Attitude to Learning Policy and Anti-Bullying Policy and reviewed on an annual basis to ensure current Government guidance, new initiatives and technological and internet developments are considered. Online Safety incidents, where they occur, will also inform this policy where necessary. The Online Safety Coordinator and Deputy Data Protection Officer (DPO), **Lewis Thompson** will actively monitor and evaluate the Online Safety policy, with input from school staff and external agencies, including, but not limited to:

- Head teacher and school leadership team **Domenic Volpe / SLT**
- DPO **Maxine Webb**
- School staff
- Network manager **Aspire Technology Solutions (Managed Service Provider)**
- IT Technical Support **Lauren Clarke**
- External IT contractors, e.g. web developer, e-learning provider **Google**
- Governor(s) **Tracey Johnson**
- Students, e.g. a member of the student council **Student Ambassadors**
- Designated Safeguarding Lead **Claire Richardson**

In the event of an Online Safety incident, the following people will be informed within school and in external agencies and stakeholder organisations: **Lewis Thompson, Claire Richardson, Domenic Volpe, Maxine Webb**.

The Online Safety policy will be reviewed on an annual basis and promptly upon:

- Serious breaches of the policy
- New guidance by Government/LEA/safeguarding authorities
- Significant changes in technology as used by the school or students in the wider community
- Online Safety incidents in the community or local schools which might impact on the school community
- Advice from the police

The school Online Safety Coordinator:

The school's designated Online Safety Coordinator reports to SLT and governors and co-ordinates Online Safety provision across the school. The Online Safety Coordinator is responsible for staff and student training, ensuring needs are met and the responsibilities of both groups are transparent and explicit.

Although all staff are responsible for upholding the school Online Safety policy, Aspire Technology Solutions (Managed Service Provider) and the school IT Technical Support are responsible for monitoring internet use by students and staff onsite, and on school machines such as laptops used off-site. The current filtering and monitoring system managed by Aspire Technology Solutions is Smoothwall.

The Online Safety Coordinator is the first point of contact in an online safety incident and is responsible for acting as a point of contact for support and advice on online safety issues.

Governors' responsibility for Online Safety:

At least one governor is responsible for online safety. The school Online Safety Coordinator will liaise with the governing body on online safety issues and ensure appropriate training is given.

Teaching and support staff

Staff will ensure that they are aware of the current school online safety policy and procedures. Staff must rigorously monitor pupil internet and computer use in line with the policy. This includes the use of personal technology such as cameras, phones and other gadgets on the school site.

Staff are expected to use internet technology provided to them by the school for teaching and learning purposes only and ensure that school email accounts are only used for school related business.

Staff will ensure that any photographs taken of students (during learning activities) on a personal device (digital camera, tablet, mobile phone) should be uploaded to the school network/school Google Drive account as soon as possible and should be deleted from the device, removable storage (SD card) and any linked personal cloud storage.

External storage (USB sticks, external hard drives, SD cards) should not be used to store school work and information. Staff should only access work and school information off site through their Google Drive and/or school network account.

School has been informed, via parents/guardians of students who may not be photographed (for safeguarding reasons etc.) and staff are made aware of this.

Staff are expected to protect their professional integrity online when using social media and should ensure that all social media accounts are made private. Staff should not use social media to communicate with current students or past students under the age of 18. Staff should only use authorised school accounts to post information to parents and students and should not give their home address, phone number, mobile number, personal social networking details or email address to students or parents. All communication with parents should be done by authorized school contact channels.

Staff should ensure that any personal mobile device in their possession is used discreetly when in school and only when necessary.

Remote Learning - Staff

In the event that staff are required to work from home, they should ensure that they continue to follow the guidelines set out in this policy.

- Use only school approved platforms for learning opportunities (Google Classroom/Google Drive)
- Use only school approved platforms for staff/department meetings (Google Meet)
- Use only school approved platforms to contact students (GMail/Google Classroom) and parents (GMail, telephone). All contact should be formal and school related.
- Use only school approved platforms to contact parents (GMail).
- Personal email addresses and phone numbers should not be shared with students or parents and staff phone numbers should be hidden using privacy settings if contacting parents by phone.

Designated Safeguarding Lead

The Designated Safeguarding Lead is able to differentiate which Online Safety incidents are required to be reported to CEOP, local police, LADO, social services and parents/guardians. The individual will also determine whether the information from such an incident should be restricted to nominated members of the leadership team.

Students

Students are expected to use internet technology provided to them by the school for learning purposes only and respect and look after any equipment in their use. If internet technology is used in an unacceptable manner the student may have their right to access the school system revoked or limited and in severe cases may be isolated and/or excluded. The school reserves the right to monitor, record or delete any data or software on student accounts.

Students' internet use out of school on social networking sites such as Facebook is covered under this policy if it impacts on the school and/or its staff and students in terms of cyber-bullying, reputation or illegal activities.

Students are aware of how to report Online Safety incidents in school, and how to use external reporting facilities, such as the CEOP report abuse button.

Students are expected to keep themselves safe online by keeping personal information private (including their passwords), blocking inappropriate messages and informing staff of any unacceptable use. Unacceptable uses of ICT are, but are not limited to:

- Using disrespectful or offensive language
- Cyberbullying
- Risking their own personal safety
- Identity theft
- Playing inappropriate games
- Participating in unauthorised chat rooms
- Social networking or instant messaging
- Opening, reading or sending inappropriate emails or texts (sexting)
- Not adhering to copyright rules

Remote Learning - Students

Students are expected to follow the guidelines set out in this policy both at school and in a remote learning environment, should such a situation occur. In the event of a student or students having to work from home, they must use ICT appropriately as they would be expected to in a school setting. Students should:

- Use online platforms and email appropriately:
    - Write and speak as they would in class and avoid "text" speak
    - Ensure all communication with teaching staff is school related, respectful and polite
    - Only communicate through school approved platforms, such as GMail and Google Classroom.
    - Avoid using school platforms to discuss personal matters
- Take regular screen breaks where appropriate
- Use the School Worry Wall on the school website to report any safeguarding concerns

Mobile Phone Use (Other Personal Devices)

We strongly advise that students do not carry their mobile phones with them at school or on school trips, but we accept that parents may wish that their child carries a mobile phone when travelling to and from school for use in an emergency. However, both parents and students agree that mobile phones will be kept switched off and not used while on the school premises.

Students found using mobile phones or other personal devices, inappropriately or in contravention of agreed policy, within school will have their device confiscated which must then be collected from the Support Zone at the end of the school day.

Where a mobile or other device is brought into school, it is entirely at the students' and parents' own risk. The school accepts no responsibility for the loss, theft or damage of any phone or other electronic device.

It is forbidden to record photographic images (still or video) or sound recordings of staff or students at any time using a personal device, mobile phone, tablet or other recording equipment.

The school reserves the right to search the content of a confiscated device where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Consequences of Misuse of ICT

If a student does not follow the stipulations indicated in this policy they will be held to account by their Head of Key Stage.

Parents and guardians

Parents and guardians are expected to support the school's stance on promoting good internet behaviour and responsible use of ICT equipment both at school and at home.

The school will provide opportunities to educate parents with regard to Online Safety, including:

- Parents' evenings, open days, transition evenings, or other events to take advantage of occasions when there are large numbers of parents in school.
- Online Safety information delivered to parents directly or via the school website/social media feeds.

Guidance for other users

External users with significant access to school systems including sensitive information or information held securely under the Data Protection Act should be DBS-checked. This includes external contractors who might maintain the school domain name and web hosting, which would facilitate access to cloud file storage, website documents and email.

How does the school provide Online Safety education?

- Online Safety events, e.g. Safer Internet Day and Anti-Bullying Week.
- Online Safety as part of pastoral care including: form time activities; assemblies; year group presentations; tutorial opportunities.
- Online Safety taught during collapsed timetable days teaching: how to deal with cyber-bullying; how to report cyber-bullying; the social effects of spending too much time online; how to judge the validity of website information; how to remove cyber-bullying; computer usage and the law; how to spot and remove viruses; why copyright is important.
- Online Safety posters are displayed prominently around school.

External Agencies

- External agency visitors should be made aware of the school Online Safety Policy and procedures.
- Visitors coming into school must agree to refrain from using devices to take photographs of students, unless arranged with the business manager. Guest WiFi is available to visitors, but access to this is limited and monitored by Aspire Technology Solutions.

Documents to be referred to:

- Sexting in Schools and Colleges 2016 - UKCCIS
- Keeping Children Safe in Education 2020 - DfE

This policy should be read in conjunction with other school policies:

- Remote Learning Policy
- Attitude to Learning and Behaviour Policy and Procedure
- Child Protection and Safeguarding Policy
- Data Protection Policy