Kingsmeadow
Community School

ONLINE SAFETY POLICY

Updated October 2017

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 gender, ethnicity, religion, sexuality, age or any disability.

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 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 the 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 Behaviour Watch.

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 Behaviour Watch.

3. Safeguard the rights and freedoms of others. We must actively pursue our aim to help pupils 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 Behaviour Watch.
- 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 pupils are not excluded from activities because of status or income.

Success Criteria

- All student groups are able to access the curriculum fully and discrete intervention results in specific gaps in student achievement narrowing and in line with the whole school population and national figures. Eg boys, girls, students with SEND and students receiving free school meals.

Online Safety Policy

Internet technology helps pupils 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.

Pupils, 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 at school. This can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a blacklist of prohibited activities; it is a list of areas to discuss, teach and inform. It will develop positive behaviour and knowledge leading to safer internet use and year-on-year improvement, with a measurable impact on Online safety. The positive effects of the policy are intended to be seen online and offline in school and at home, and ultimately beyond school and into the workplace.

Online Safety Policy scope

The school Online Safety policy and agreements apply to all pupils, staff, support 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 school will make reasonable use of relevant legislation and guidelines to effect positive behaviour regarding ICT and internet use on and off the school site. This will include imposing rewards and sanctions for behaviour and penalties for inappropriate behaviour as defined as 'regulation of student behaviour' under the Education and Inspections Act 2006. 'In loco parentis' provision under the Children Act 1989 allows the school to report and act on instances of cyber-bullying, abuse, harassment, malicious communication and grossly offensive material. This includes reporting to the police, social media websites, and hosting providers on behalf of pupils.

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, e-learning platforms, blogs, social media websites
- External access to internal school networking such as webmail, network access, file-serving (document folders) and printing
- Pupils' and staff's personal ICT equipment when used in school and which makes use of school networking, file-serving or internet facilities
- Mobile phones when used on the school site under the supervision of staff

Reviewing and evaluating Online Safety and ensuring good practice

Online Safety policy results from a continuous cycle of evaluation and review based on new initiatives and partnership discussion with stakeholders and outside organisations, technological and internet developments, current Government guidance and school-related Online Safety incidents. The policy development cycle develops good practice within the

teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses helps to determine inset provision for staff and governors and guidance for parents, pupils and local partnerships.

The Online Safety committee will actively monitor and evaluate the Online Safety policy. This committee will comprise:

- Online Safety co-ordinator/officer **Lewis Thompson**
- Head teacher and school leadership team **Domenic Volpe**
- Teaching staff
- 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**
- ICT technical support and network manager SCS (Managed Service Provider)
- External IT contractors, e.g. web developer, e-learning provider **Realsmart**
- Governor(s) **Cllr Allison Thompson**
- Parents and guardians, e.g. PTA, parent governors, looked-after children/social care representatives
- Pupils, e.g. a member of the student council **Student Voice**
- 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.

When will your Online Safety policy and acceptable use policies be 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 Online Safety incidents
- New guidance by Government/LEA/safeguarding authorities
- Significant changes in technology as used by the school or pupils in the wider community
- Online Safety incidents in the community or local schools which might impact on the school community
- Advice from the police

Where will the Online Safety policy review be documented?

- In the school development plan

This provision will be evidenced in the following school document(s):

Staff, parent and pupil Online Safety audits and pupil questionnaires will inform Online Safety learning and staff training requirements. This will gauge the impact and effectiveness of the Online Safety provision and determine future Online Safety targets.

Policy review schedule

- This policy was approved by Kingsmeadow School Governing Body on September 2017. It is stored here: http://kingsmeadow.org.uk/school-policy-documents/ and is published for viewing by parents and the wider school community here: www.kingsmeadow.org.uk.
- The Online Safety policy will be monitored Annually. The next review date is: September 2018.
- The Online Safety policy will be reviewed and evaluated promptly in the light of serious Online Safety incidents. The last recorded serious Online Safety incident was on . As a result this policy was reviewed on .
- The Online Safety policy will be reviewed and evaluated promptly in the light of important changes to legislation or Government guidance related to Online Safety. The last recorded such change was on and as a result this policy was reviewed on .

The Online Safety co-ordinator/officer will include evidence of evaluations of the impact of the Online Safety policy in reports. Such evidence includes (tick the boxes you wish to include):

- Statistics of filtering breaches
- Logs of internet and network traffic activity
- Online safety audits of staff, support staff, parents, governors and other stakeholders
- ParentView and/or Ofsted questionnaire results

The governing body/proprietor will receive a report on the progress, evaluation, impact and effectiveness of the Online Safety policy annually. This report will include suitably redacted Online Safety incident accounts and statistics, detailing how they have been resolved, and the countermeasures that were implemented.

School management and Online Safety

School senior management is responsible for determining, evaluating and reviewing Online Safety policies. This encompasses teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors. It also includes agreed criteria for acceptable use by pupils, school staff and governors of internet-capable equipment for school-related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

Online Safety provision is always designed to encourage positive behaviours and practical real-world strategies for all members of the school and wider school community.

Management is encouraged to be aspirational and innovative in developing strategies for Online Safety provision which will deliver measurable success via a calendar of Online Safety provision. Management should clearly state Online Safety targets with success criteria on the school development plan.

Evidence base:

- School development plan
- Minutes from Online Safety-related meetings with staff, SLT, parents association, governors and wider school community stakeholders
- Regularly updated Online Safety policy, child protection policy and logged and evaluated Online Safety incidents
- Staff inset provision audit and record

The school Online Safety Co-ordinator

The school's designated Online Safety Co-ordinator, Lewis Thompson, reports to SLT and governors and co-ordinates Online Safety provision across the school and wider school community.

Although all staff are responsible for upholding the school Online Safety policy and implementing safer internet practice, SCS (Managed Service Provider), are responsible for monitoring internet use by pupils and staff onsite, and on school machines such as laptops used off-site. The current filtering and monitoring system managed by SCS is Smoothwall. Lewis Thompson is responsible for monitoring internet use on Google Chromebooks while at home, using the GoGuardian programme.

- The Online Safety Co-ordinator is responsible for promoting best practice in Online Safety within the wider school community, including providing and being a source of information for parents.
- The school Online Safety Co-ordinator audits and assesses inset requirements for staff, support staff and governor Online Safety training, ensuring that all staff are aware of their responsibilities and the school's Online Safety procedures. The Coordinator is the first port of call for staff requiring advice on Online Safety matters.

The Co-ordinator:

- Is the first point of contact in an Online Safety incident
- Is responsible for acting as a point of contact for support and advice on Online Safety issues.
- Is responsible for promoting Online Safety awareness for parents and wider stakeholders.
- Is responsible for ensuring staff receive information about current trends.
- Is responsible for managing Online Safety training for all staff.
- Is responsible for ensuring the Acceptable Use Policy is in place, agreed by staff, pupils and parents and are monitored, evaluated and reviewed.
- Is responsible for ensuring the Online Safety Policy is adhered to.
- Is responsible for ensuring that the Online Safety Policy links with other appropriate school policies, e.g. anti-bullying, child protection, ICT, PSHE.
- Is responsible for evaluating and reviewing the school's Online Safety Policy, updating at least annually.
- Is responsible for promoting a school and community-wide Online Safety culture and promoting the school's Online Safety vision.

Governors' responsibility for Online Safety

At least one governor is responsible for Online Safety. The school Online Safety Co-ordinator will liaise directly with the governor about reports on Online Safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community.

The Online Safety Co-ordinator will be responsible for auditing governor Online Safety training and inset requirements.

Teaching and teaching support staff

Teaching and teaching support staff ensure that they are aware of the current school Online Safety Policy, practices and associated procedures for reporting Online Safety incidents.

Teaching and teaching support staff will be provided with an Online Safety induction as part of the overall staff induction procedures.

All staff must ensure that they have read, understood and signed (thereby indicating an agreement) the acceptable use policies relevant to internet and computer use in school.

All teaching 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.

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

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

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.

The Designated Safeguarding Lead knows how to deal appropriately with incidents including (but not limited to):

- Allegations against members of staff
- Computer crime, e.g. hacking of school systems
- Allegations or evidence of 'grooming'
- Allegations or evidence of cyberbullying in the form of threats of violence, harassment or a malicious communication.

Pupils

Pupils are required to use school internet and computer systems in agreement with the terms specified in the school's Acceptable Use Policy. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.

Pupils 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.

Pupils are aware that school acceptable use policies cover all computer, internet and gadget usage in school, including the use of personal items such as phones.

Pupils are aware that their internet use out of school on social networking sites such as Facebook is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and pupils in terms of cyber-bullying, reputation or illegal activities.

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 both at school and at home.

The school expects parents and guardians to sign the school's acceptable use policies, 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 arrangements, questionnaires and the VLE.

Parents

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, including: letters, newsletters, parentmail, website-subscribed news emails, the school extranet, learning platform, website or VLE.

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 CRB-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?

Possible curriculum opportunities:

- 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 L4L days teaching (but not limited to): 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.

Wider school community and stakeholders

Possible information dissemination opportunities:

- Open days or other events to take advantage of occasions when there are large numbers of visitors in school.
- Online Safety information delivered to stakeholder directly, including: letters; newsletters; website-subscribed news emails; school extranet; learning platform; website; or VLE.

Staff – inset and training

- Online Safety information directly delivered to staff including: letters; newsletters; website-subscribed news emails; school extranet; learning platform; website; or VLE.
- The Online Safety Policy will be updated and evaluated by staff at the beginning of each academic year.
- The Online Safety Coordinator (**Lewis Thompson**) should be the first port of call for staff requiring Online Safety advice.

Governors – training

Possible training and information dissemination opportunities:

- Open days or other events to take advantage of occasions when there are large numbers of visitors in school.
- Online Safety information delivered to governors directly including: letters; newsletters; website-subscribed news emails; school extranet; learning platform; website; or VLE.

IT support staff - contractors, filtering and monitoring

Possible training and information dissemination opportunities:

- IT technical support staff and network managers should have relevant industry experience and Microsoft/Cisco-certified qualifications.
- Support staff and contractors need to be CRB-checked and agree to and sign the school's Online Safety AUP for visitors.
- IT technical support staff and onsite contractors (cleaners, maintenance workers) are all given pertinent child protection and Online Safety, which is reviewed annually.
- 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 SCS.