KINGSLAND SCHOOL

COMPUTING & ONLINE SAFETY POLICY



POLICY UPDATED JANUARY 2024

Introduction

The Kingsland Computing & Online Safety Policy encompasses a number of Wakefield Council policies regarding the use of technology, electronic equipment and online safety. This policy meets the 'spiritual, moral, social and cultural development' values held by Kingsland School. It sets out the principles for all Kingsland School staff and visitors in regards to the use of electronic equipment and technology within school.

This policy is also based on the DfE guidance 'Teaching online safety in schools' (January 2023).

Any further information regarding aspects of the Kingsland Computing Policy can be found through the following policy documents -

Code of Conduct
Electrical Use
WMDC Model Social Media Policy for School Employees (2014)
Behaviour
Anti-Bullying
Curriculum planning documents for Computing and PSED including Relationships Education
Data Protection
Safeguarding and Child Protection

Definition/Aims

At Kingsland School, all children are supported to access technology at their level, to practise and embed keys skills, and to develop an understanding of the safe use of a variety of technological resources. This policy reflects how this is achieved for the wide range of learners at Kingsland School.

Online Safety (formally E-Safety) encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguarding and awareness for users to enable them to control their online experiences.

The school's Online Safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Computing Curriculum, Data Protection, Safeguarding and Child Protection. This policy outlines our purpose in providing e-mail facilities and access to the internet and explains how the school is seeking to avoid the potential problems that unrestricted internet access could give rise to. The Online Safety co-ordinator is the Headteacher. The policy has been written by the school, building on the Wakefield and Government guidance. It has been agreed by all staff and approved by the Governing Body.

Philosophy & Intent of Computing at Kingsland

At Kingsland School we realise how prevalent the use of digital technology is within each aspect of everyday life and, therefore, how essential it is that our children develop skills that enable them to use and access everyday technologies as independently as possible. We are passionate that the computing curriculum reflects the delivery of lessons that promote key life skills, learning through each child's personal interests and developing cross-curricular skills, such as, spelling, reading and key communication skills.

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Virgin Media via Smarter Solutions (Castleford Site), Talk Talk via Vapour Media Limited (Stanley Site) protected with Smoothwall filtering.

Providing access to the Internet in school raises educational standards and supports the professional work of staff. Teachers and pupils will have access to web sites offering educational resources, news and current events in order to access opportunities. There will be opportunities to communicate and exchange information with others. In addition, staff will have the opportunity to access educational materials and good curriculum practice; to communicate with the advisory and support services, professional associations and colleagues; to exchange curriculum and administration data with the LA and DfE; to receive up-to-date information and participate in government initiatives. The Internet will also be used to enhance the school's management information and business administration systems.

Enabling Access/Equal Opportunities

Teachers support inclusive practice by applying the three inclusion principles:

- setting suitable learning challenges
- responding to pupils diverse needs
- overcoming potential barriers to learning and assessment for individuals and groups of pupils.

We make computing accessible to pupils by:

- being aware of individual needs and learning objectives
- using events, objects and multisensory resources that are relevant, motivating, of a high quality and enjoyable
- incorporating computing technology into everyday tasks where possible
- emphasising relevant computing vocabulary and modelling its use in concrete situations
- introducing new skills and concepts by building on those that are well-established
- modelling how to successfully use a range of software, hardware and other technological resources

- recognising potentially motivating contexts and using them to support the consolidation and extension of learned skills
- encouraging peers to interact with each other and adults
- allowing pupils time to respond and communicate
- balancing consistency and challenge
- adapting equipment, activities or the environment, or providing alternative and differentiated activities
- being aware of the pace at which pupils work and the physical effort that may be required to complete a task
- giving opportunities for the practise and retrieval of new skills.

Inclusive practice is supported by:

- involvement of other professionals e.g. SALT, OT, physiotherapists, advisory teachers for the visually and hearing impaired
- use of specialist resources e.g. switches, VOCAs
- use of specialist accommodation/environment e.g. sensory pod (Stanley), music technology pod (Stanley CLDD), computer suites (both sites)
- careful grouping and differentiation of activities
- use of staff to support and challenge
- parental involvement.

Differentiation

IEPs and individual programmes of learning reflect a pupil's particular stage of learning and current targets. Teachers are responsible for planning and implementing differentiated lessons and blocks of work, and use planning documents for the delivery of the computing curriculum that state the learning outcomes for the children in their group within each lesson.

Implementation of the Computing Curriculum

We have four curriculum pathways at Kingsland – ELF (EYFS), SLD, SCERTS and CLDD.

SLD is our only subject specific pathway beyond ELF and so this is the only main-school pathway where a discrete computing curriculum is taught. On our non-subject specific pathways – SCERTS and CLDD – the foundations of computing skills and understanding are taught through the Cognition strand of the curriculum.

ELF curriculum pathway:

Computing is embedded within all areas of the Early Years curriculum and is taught discreetly and throughout everyday learning. Progress within computing on the ELF curriculum pathway is not specifically tracked, however, evidence may be seen within pupils' learning journeys in the form of observations, children's work and photographs.

SLD (subject specific) curriculum pathway:

The National Curriculum for Key Stage One and Two for the purpose of study states that:

'A high-quality computing education equips pupils to use computational thinking and creativity to understand and change the world. Computing has deep links with mathematics, science, and design and technology, and provides insights into both natural and artificial systems. The core of computing is computer science, in which pupils are taught the principles of information and computation, how digital systems work, and how to put this knowledge to use through programming. Building on this knowledge and understanding, pupils are equipped to use information technology to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world' (DfE, 2013, p.1).

In terms of the formal teaching of computing, Kingsland School has developed its own schemes of work in Computing for SLD Lower School and Upper School classes in accordance with the National Curriculum, but in such a way that the very specific needs of pupils with severe, profound, and complex learning needs on this pathway are met.

The SLD Computing curriculum across Lower and Upper School at Kingsland is divided into three key areas. These areas are then divided further to support differentiated learning, progression and accurate assessment using the progression map statements – 'experience and explore', 'embed and recall', 'awareness and application in real life contexts'. The three key areas of the SLD Computing curriculum at Kingsland are:

Computer Science/Information Technology

This strand is delivered to meet each child's needs and interests by ensuring progression is made with the use of appropriate technological resources, visual supports and adult modelling to support children with:

- identifying sources of technology and their different parts and purposes within everyday life
- following simple instructions related to the use of technological equipment
- understanding that sources of technology follow 'instructions' to work effectively through the use of programmable toys, programmable software and cause and effect resources.

Digital Literacy

This strand is delivered to meet each child's needs and interests by ensuring progression is made with the use of appropriate technological resources, visual supports and adult modelling to support children with:

- developing typing and communication skills using technological resources
- expressing themselves using technology to make choices, make and show recordings etc
- recognising and identifying different icons and applications and using them for a purpose
- using developing skills to create documents that present information with words, pictures and videos
- developing an understanding of how the internet can be used to communicate with others through the use of email.

E-Safety

This strand is delivered to meet each child's needs and interests by ensuring progression is made with the use of appropriate technological resources, visual supports and adult modelling to support children with:

- developing an understanding what is safe and what is not
- developing an awareness of how to use the internet and who with
- developing an awareness of what personal information is
- knowing what a stranger is and that we can also encounter a stranger on the internet
- becoming confident to ask for help when using the internet.

Computing and the resources associated with this subject are particularly motivating to many children at Kingsland School. This means that the development of computing skills are easily and effectively incorporated into general routines and cross-curricular activities.

Implementation of the Online Safety policy within teaching

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. It is a part of the statutory curriculum and a necessary tool for staff and pupils. The school Internet access is designed expressively for pupil use and includes filtering appropriate to the age of the pupils. Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. At Kingsland, we know that the internet and other technologies are embedded in our pupil's lives, not just in school but outside as well. We believe that we have a duty to help prepare our pupils to safely benefit from the opportunities that the internet offers.

Online Safety is focused on within the SLD Computing Curriculum, with focus topics each term with lower and upper school. Online Safety is also addressed through the PSED curriculum on the SLD curriculum pathway. On the SCERTS and CLDD curriculum pathways, early foundations of Online Safety are taught through Cognition and PSED strands of the curriculum. This includes teaching around different types of relationships with others, giving consent and learning to say 'no', making choices and showing preferences, building trust with familiar adults, asking for help etc. Across all curriculum pathways, teaching of Online Safety is done discretely, though the whole curriculum, and children are encouraged to make the correct choices and follow guidelines when using computers and other technology. Wherever possible, Kingsland will try and take part in national campaigns, such as Safer Internet Day and plan appropriate activities for children around these themes. Child friendly search engines, such as Google Safe Search, Kiddle and Kidrex will be used when completing internet searches within planned teaching sessions.

Planning

It is the class teacher's responsibility to decide how to plan the medium term computing and online safety coverage for their particular group of pupils. This is monitored by subject leads and SMT. Class teachers are responsible for planning for the foundations of or development of computing skills for pupils in their class. Planning is done in accordance with the whole school Teaching and Learning policy.

Planning also takes account of pupils' IEPs and ILPs.

Assessment, Recording and Reporting

Progress and assessment in computing is recorded and reported on differently in each curriculum pathway. It is reported to all parents at the end of the school year through an Annual Report to Parents, the format of these also differing according to curriculum pathway. All parents receive copies of pupil IEPs/ILPs throughout the school year.

Across all curriculum pathways, teachers use a range of formative and diagnostic assessment methods, including photographic evidence, observational evidence, individual learning journeys and annotated work in pupil books/files.

Within the ELF curriculum pathway, Computing is not taught specifically and is discreetly taught within all aspects of other teaching to ensure that children are developing confidence and those first key skills with relation to technology resources. Progress within computing on the ELF curriculum pathway is not specifically tracked, however, evidence may be seen within pupils' learning journeys in the form of observations, children's work and photographs.

Within the SLD curriculum pathway, pupil progress in Computing is recorded, reported on and monitored using Progression Maps. Progression maps within the SLD curriculum pathway are used to guide teacher planning, to set individual targets for the following term and to set progress expectations by the end of either lower or upper school.

Within the SCERTS curriculum pathway, pupil progress in the Cognition strand of the curriculum is recorded, reported on and monitored using termly SCERTS assessments. Progression maps within the SCERTS curriculum pathway are used to guide teacher planning and to set individual pupil targets for the following term.

Within the CLDD curriculum pathway, computing skills are largely addressed within the Cognition strand of the curriculum, although computing skills are worked on functionally across all strands of the CLDD curriculum. Pupil progress in the Cognition strand of the curriculum is recorded, reported on and monitored using termly updates to the Quest for Learning framework and Engagement Model. Progression maps within the CLDD curriculum pathway are used to guide teacher planning and to set individual pupil targets for the following term. All pupils also have an ILP in the area of Cognition.

Ensuring Internet Access Is Appropriate and Safe

Staff, including supply staff, will not be expected to take charge of an Internet activity without training. Staff should be given opportunities to discuss the issues and develop good teaching strategies. All staff (including teachers, supply staff and teaching assistants) and any other adults involved in supervising children accessing the Internet will be provided with the school's 'Online Safety' Policy, and will have its importance explained to them. Parents' attention will be drawn to the policy in our school prospectus. Our school's Online Safety Policy will be available for parents and others to read on demand and on the school website.

The Internet is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by the teacher and the school. The school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our Internet access is purchased from Virgin Media via Smarter Solutions (Castleford Site), Talk Talk via Vapour Media Limited (Stanley Site) and a filtering system is provided by Smoothwall intended to prevent access to material inappropriate for children
- Children using the Internet will be working in the classroom, during lesson time and will be supervised by an adult at all times
- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils
- Staff will be particularly vigilant when pupils are undertaking their own search
- Where appropriate based on their learning difficulty, pupils will be taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others
- The SMT will monitor the effectiveness of Online Safety strategies
- The Headteacher will ensure that the policy is implemented effectively
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LA, our Internet Service Provider and the DfE
- The school reserves the right to delete any files that may be held on its computer system.

It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen.

The school has a set of Rules of Responsible Internet Use that pupils are taught (in ways appropriate to their learning needs). The rules are:

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- *I will only use the computers or access the internet with permission from an adult.*
- *I will ask permission before entering any website, unless my teacher has already approved that site.*
- *I will not look at or delete other people's files.*
- *I will only e-mail people I know, or my teacher has approved, and the messages I send will be polite and sensible.*
- *I will not give out my home address or phone number, email address or arrange to meet someone.*
- *I will not open emails or attachments from people I do not know.*
- *If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.*
- *I understand the school may check my computer files and will monitor the Internet sites I visit.*
- *I will respect the computer equipment.*
- *I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.*

A most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material the school will wish to respond to the

situation quickly and on a number of levels. Responsibility for handling incidents involving children will be taken by the SMT, the Designated Safeguarding Lead (Head Teacher) and the pupil's class teacher. All the teaching staff will be made aware of the incident at a staff meeting, if appropriate.

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue
- If staff or pupils discover unsuitable sites the SMT will be informed. The school will report the URL (address) and content to the Internet Service Provider and the LA; if it is thought that the material is illegal, after consultation with the ISP and LA, the site will be referred to the Internet Watch Foundation and the police.

Where appropriate, pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use, which have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet or use of e-mail facilities by failing to follow the rules they have been taught or failing to follow the agreed search plan when given the privilege of undertaking their own Internet search, then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers. Teachers may also consider whether access to the Internet may be denied for a period.

Managing Internet Access

Information system security:

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the Local Authority

E-mail:

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive an offensive e-mail
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission

Published content and the school web site:

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office
- The Headteacher will take overall responsibility and ensure that content is accurate and appropriate

Publishing pupils' images and work:

- Photographs that include pupils will be selected carefully so that the image cannot be misused
- Pupils' full names will not be used anywhere on the school web site or other online space, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site
- Work can only be published with the permission of the pupil and parents/carers

Social networking and personal publishing:

- The school will control access to social networking sites and consider how to educate pupils in their safe use
- Newsgroups will be blocked unless a specific use is approved
- Pupils will only be permitted to use moderated social networking sites

Managing filtering:

- The school will ensure systems are in place to protect pupils

- If staff or pupils come across unsuitable online materials, the site must be reported to the Online Safety Co-ordinator (the Headteacher).

Managing emerging technologies:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- The SMT should be aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications
- Mobile phones will not be used during lessons or in areas whilst pupils are present
- Staff will have access to a school phone where contact with pupils or parents is required
- Staff are not permitted to use personal mobile phones to take photographs
- Staff must inform a member of the SMT if photographs of pupils are being taken off the school site for editing
- Staff must not publish photographs of pupils on the Internet - Staff must be aware of children's photograph permissions

Protecting personal data:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and will follow GDPR guidelines

Policy Decisions & Implementation

Authorising Internet access:

- All staff must read and sign the Online Safety Policy before using any school ICT resources
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems
- Pupil access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials

Assessing risks:

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor LA can accept liability for any material accessed, or any consequences of Internet access

Handling Online Safety complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.

Introducing the Online Safety policy to pupils:

- Online Safety rules will be posted in all rooms where computers are used and discussed with pupils
- Posters displaying online safety advice and helplines will be posted in all rooms where computers are used and discussed with pupils
- Pupils will be informed that network and Internet use will be monitored
- Online Safety training for individual pupils will be developed according to the needs of each pupil

Staff and the Online Safety policy:

- All staff will be given the school's Online Safety policy and its importance explained

Enabling Access/Equal Opportunities:

Where appropriate, pupils will learn how to use a web browser. Older pupils will be taught to use suitable web search engines. Staff and pupils will begin to use the Internet to find and evaluate information. Access to the Internet will become a planned part of the curriculum that will enrich and extend learning activities and will be integrated into the schemes of work.

As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use.

Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the Internet may be by teacher (or sometimes other adult) demonstration
- Pupils may access teacher-prepared materials, rather than the open Internet
- Pupils may be given a suitable web page or a single web site to access
- Pupils may be provided with lists of relevant and suitable web sites which they may access

An adult, normally their teacher, will supervise pupils accessing the Internet at all times. They will only be allowed to use the Internet once they have been taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the Internet.

Curriculum content/Using information from the Internet:

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the Internet is intended for an adult audience, much of the information on the Internet is not properly audited/edited and most of it is copyright.

Pupils will be taught:

- to expect a wider range of content, both in level and in audience, than is found in the school library or on TV
- to observe copyright
- to be aware that information on the internet might be opinion and not fact
- of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet
- in the safe use of ICT
- that the writer of an e-mail or the author of a web page may not be the person claimed
- what positive, healthy and respectful online relationships look like
- about the effects of their online actions on others
- how to recognise and display respectful behaviour online
- how to use technology safely, responsibly, respectfully and securely
- where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- the ways in which someone may put themselves at risk online
- risks posed by another person’s online behaviour
- when risk taking can be positive and negative
- online reputation and the positive and negative aspects of an online digital footprint
- sharing information online and how to make a judgement about when and how to share and who to share with
- the risks of cyber crime, online fraud and identity theft
- when someone might be using persuasive techniques online and what to do about this

Using e-mail:

Where appropriate, pupils will learn how to use an e-mail application and be taught e-mail conventions. Staff and pupils will begin to use e-mail to communicate with others, to request information and to share

information. It is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

- Pupils will only be allowed to use e-mail once they have been taught the Rules of Responsible Internet Use and the reasons for these rules
- Teachers will endeavour to ensure that these rules remain uppermost in the pupils' minds as they monitor pupils using e-mail
- Pupils may send e-mail as part of planned lessons
- In-coming e-mail to pupils will not be regarded as private
- Pupils will have the e-mail messages they compose checked by a member of staff before sending them
- The forwarding of chain letters will not be permitted.

Opportunities to develop Spiritual, Moral, Social And Cultural Development:

The school ethos promotes SMSC development and this permeates throughout the whole curriculum. The use of the Internet makes a particular contribution to the development of SMSC development by enabling access to information worldwide.

Monitoring, Evaluation and Development Planning

The subject co-ordinator(s), supported by the Senior Management Team, is/are responsible for monitoring the subject. Governors should ensure that monitoring and evaluation are carried out.
The subject co-ordinator(s) will monitor the following aspects in order to produce a subject audit as part of the whole school self-review and evaluation process:

- Policy and scheme of work/curriculum – annually
- Resources – on a regular basis in order to ensure quantity, quality, accessibility and use
- Teachers' planning – long term plans once a year, medium term plans once a term, short term plans on request
- Staff expertise in the subject – through the professional development programme, feedback from teachers attending courses relevant to the subject, professional development of the co-ordinator(s), performance management systems
- Assessment – on a termly basis through planning, sampling of teacher records as part of the yearly monitoring process
- Quality of pupils' work – through viewing displays, portfolios, informal discussions, systematic sampling as part of the yearly monitoring process (moderation meetings core subjects) and as part of performance management cycles
- Classroom practice – on a yearly basis and as part of performance management cycles to monitor and evaluate the quality of teaching, pupil response and attitude, and pupil learning.

The co-ordinator(s) is/are responsible for completing an annual action plan as a result of the findings of the above audit, which will inform the School Development Plan.

The Kingsland School website

Our school website intends to:

- Provide accurate, up-to-date information about our school
- Celebrate achievements
- Promote the school

Adults identified by the SMT are responsible for uploading pages to the school website and VLE, ensuring that the links work and are up-to-date, and that the sites meet the requirements of the site host. The point of contact on the web site will be the school address, telephone number and e-mail address. Home information or individual e-mail identities will not be published. Permission will be sought from other individuals before they are referred to by name on any pages we publish.

Internet Access and Home/School Links:

We will keep parents in touch with future ICT developments by letter and newsletter. Internet use in pupils' homes is rapidly increasing and some parents may be grateful for any advice/guidance that school can offer – especially with regard to safe access for children. Further:

- Parents can send photographs or information relating to their child to the given email address as created by the Computing Co-ordinator. Any emails must be permanently deleted from the mail client when used, and information downloaded must be stored safely. Any inappropriate emails sent to these emails addresses must be shown to the Online Safety Co-ordinator. Staff must ensure any reply to an email is done in a professional manner and they must not use their personal work email to do so.
- School guidelines on issues such as safe Internet use will be made available to parents together with printed information and Internet sites providing information for parents about safe access for children
- The school is working with parents to identify suitable educational and leisure activities for use at home

Use of Social Media for Staff

This policy is based on the 'WMDC Model Social Media Policy for School Employees' (2014).

The Internet provides a range of Social Media tools that allow users to interact with one another, for example Facebook, Twitter, mobile phone applications such as Snapchat and internet encyclopaedias such as Wikipedia. This definition of Social Media is not exhaustive as technology develops with new ways of communicating advances every day. For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

While recognising the benefits of these media as new opportunities for communication, this policy sets out the principles that staff are expected to follow when using social media. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of young people, staff and the reputation of the school are safeguarded.

Staff members also must be conscious at all times of the need to keep their personal and professional lives separate. It is important to protect everyone from allegations and misinterpretations which can arise from the use of social networking sites. Safeguarding children is fundamental to everything we do at school and it is essential that everyone considers this and acts responsibly if they are using social networking sites out of school. This policy guidance relates to social networking inside and outside of work.

The following are considered unacceptable at Kingsland School:

1. The use of the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.

2. The unauthorised posting of any images of employees, pupils, governors or anyone directly connected with the school whilst engaged in school activities.

3. The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments, discrimination, breaches of copyright, data protection or anything else that could lead to a claim for damages and/or bring the school into disrepute.

4. The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.

5. Staff members must not have any contact with pupil or their family members through their personal social media, as that contact are likely to constitute a conflict of interest and may breach professional boundaries and relationships. The Headteacher must be informed of any personal relationships with pupils and their families outside of school.

7. The use of social media to discuss, advise or make references to any matters related to school activities/business, staff, pupils, parents or governors.

8. Any actions that breaches the school's code of conduct.

Staff should be aware that if their out-of-work activity causes potential embarrassment for the school or detrimentally effects the school's reputation then Kingsland School is entitled to take disciplinary action. Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment. The use of mobile phones during break and lunchtime must be limited to the areas that are not used by pupils, for example, staff rooms. No school computers are to be used to access social networking sites at any time of day. Staff must read the 'Personal Use of Electrical Equipment Policy' and 'Acceptable Use Agreement' and abide by the guidelines.

If the Headteacher receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner as detailed above they will:

1. Record the disclosure in line with the school's safeguarding and child protection policy

2. Refer the matter to the Local Authority and/or the police as appropriate.

a. If the disclosure has come from a parent then explain processes that will be followed.

b. If disclosure comes from a member of staff then try to maintain confidentiality.

c. If disclosure is from a child, follow then follow the process described in the safeguarding and child protection policy until the police investigation has been carried out.

Personal Use of Electrical Equipment

The Personal Use of Electrical Equipment document is governed by the Acceptable Use Guidance.

Failure to maintain portable electrical equipment adequately is a major cause of electrical accidents. Equipment used in the school should be purchased by the school and will be maintained and PAT tested as appropriate in accordance with the Electricity at Work Regulations 1989.Personal electrical or electronic device are used at the owner's risk. It is the user's duty to be responsible in the upkeep and protection of the device. Kingsland School will not be responsible for personal devices which are damaged or lost whilst at school. The School will not provide support for personal devices. Any personal devices must only be used at allocated break times during the working day and away from pupils (for example, within a staff room).

Kingsland school ICT systems must be used in a responsible way, to ensure that there is no risk to a person's safety or to the safety and security of the ICT systems and other users. Abuse of the Electronic Equipment Policy is misconduct/gross misconduct and can result in immediate dismissal.

Staff, Governor and Visitor Acceptable Use Guidelines

ICT and the related technologies such as email, the internet and tablets are an expected part of our daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this policy, confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the Headteacher or Computing/Online Safety coordinator.

- I will only use the laptop and any other assigned technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords/codes provided to me by the school or other related authorities.
- I will only use the approved email system for any communications of a work-related nature and will not set up any additional email accounts without seeking permission from the Headteacher. This may include individual work email accounts and the school's approved generic email accounts which are as follows:
    - eyfskingsland@gmail.com
    - clddkingsland@gmail.com
    - ks1kingsland@gmail.com
    - ks2kingsland@gmail.com
    - kingslandsmtcontact@gmail.com
    - kingslandhomelearning@gmail.com

- I will ensure that all electronic communications with staff are compatible with my professional role.
- I will not give out my own personal details or personal information of any nature to pupils' families (including 'being friends' on social media).
- I will ensure that children's personal data (such as data held on the administration system) is kept confidential, secure and is used appropriately.
- I will only take my assigned laptop and other assigned equipment out of school for professional use and keep all data confidential and secure. All other school technologies must be left unless authorised by the Headteacher or Computing/Online Safety coordinator.
- I will ensure that the asset numbers of devices are signed out for pupil use and signed back in promptly.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher in line with data security policy.
- I will not use assigned equipment for personal use or reasons.
- I will not store any communications of a work-related nature on any personal devices.
- I will not install any hardware or software on school equipment without the permission of the Headteacher or Computing/Online Safety coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will report any accidental access to inappropriate materials immediately to the Headteacher.
- I will ensure that websites and online do not contain offensive or inappropriate content before their use in the school environment.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
- I will support and promote the school's Computing/Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the Headteacher.
- The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of all e-mail accounts and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Please also refer to the school's GDPR policy for further information.

I understand that I must read, understand and agree (via CPOMS) with this Acceptable Use Agreement and agree to support the safe use of ICT throughout the school. I understand that serious abuse of the Electronic Equipment Policy is misconduct/gross misconduct and can result in immediate dismissal.