The Kingston Academy

Online safety and Acceptable Use of ICT Policy

March 2018

Date approved: 12 March 2018
Approved by: Pupil Welfare and Community Committee
Frequency of review: Annual
Last review: September 2017
Next review due: March 2019

Contents

ONLINE SAFETY AND ACCEPTABLE USE OF ICT POLICY

Key Details	
Designated Safeguarding Lead/Online Safety Lead	**Anthony Sheppard, Assistant Head Teacher**
Lead Trustee for Safeguarding	**Sue Conder**

1. AIMS AND POLICY SCOPE

The purpose of this online safety policy is to:

- Clearly identify the key principles expected of all members of the school community with regards to the safe and responsible use of information and communication technology (ICT) to ensure that The Kingston Academy is a safe and secure environment.
- Safeguard and protect all members of the school community online.
- Raise awareness with all members of the school community regarding the potential risks as well as benefits of technology.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the school community.

This policy applies to all staff including trustees, volunteers, visitors, external contractors, and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as to pupils and parents/carers. It applies to all access to the internet and use of school ICT systems, both in school (including from personal devices) and out of school where actions relate directly to school set activity or use of school online systems or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as Chromebooks, work laptops or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) the Safeguarding and Child Protection Policy, Anti-bullying Policy, Behaviour Discipline Exclusions Restraint and Searches Policy, Mobile Phone and Personal Devices Policy (**to be adopted shortly)**, Sexting Policy, Statement on the Prevention of Radicalisation and Extremism and Staff Behaviour and Code of Conduct (copies are available on the policy page of the school website and in the policy folder on the Whole School Team Drive).

2. BACKGROUND

We encourage and support the positive use of ICT to develop curriculum and learning opportunities and we provide a curriculum that prepares pupils for the digital world. We also recognise that it is essential that the use of ICT and online tools are managed carefully to ensure that all members of our community are kept safe and protected from potential harm online.

The Department for Education guidance Keeping Children Safe in Education (September 2016) highlights online safety as a safeguarding issue for schools and identifies three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful online interaction with other users; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

This policy has been drafted with regard to that guidance and the implementation of this policy forms part of the school's safeguarding responsibilities.

We recognise that there are no totally effective solutions to moderate and control the internet, pupils and staff cannot be completely prevented from being exposed to online risks and so we have adopted an approach which incorporates both the use of regulation and technical solutions and the education of pupils and staff to take a responsible approach to online safety and to manage risk.

3. MONITORING AND REVIEW

- The Kingston Academy will review this policy at least annually and the policy will also be revised following any national or local policy requirements, any safeguarding or child protection concerns or any changes to the technical infrastructure of the school.
- We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the head teacher will be informed of online safety concerns, as appropriate.
- The named trustee for safeguarding will report on a regular basis to the Trust Board on any online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

4. ONLINE SAFETY AND RESPONDING TO A DISCLOSURE OR SAFEGUARDING CONCERN

The welfare and safety of pupils are the responsibility of **all** staff in school and any concern for a pupil's welfare MUST always be reported to the Designated Safeguarding Lead in accordance with the Safeguarding and Child Protection Policy.

5. ROLES AND KEY RESPONSIBILITIES

- The school has appointed Anthony Sheppard, as Designated Safeguarding Lead to be the online safety lead.
- The Kingston Academy recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

5.1. The Senior Leadership Team will

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety, including acceptable use agreements for staff and pupils.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.

- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

5.2. The Designated Safeguarding Lead (DSL) (supported by the Online Safety Committee) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Senior Leadership Team and to the Trust Board.
- Work with the Senior Leadership Team to review and update online safety policies on a regular basis (at least annually) with appropriate stakeholder input.
- Meet termly with the trustee with the lead responsibility for safeguarding.

5.3. The Online Safety Committee

The committee meets termly and consists of:

- The designated Online Safety Lead /Designated Safeguarding Lead;
- The Digital Learning Strategic lead
- The operations team manager
- A member of the Senior Leadership Team

5.4. It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies, through questionnaires and the Staff Consultative Committee.
- Read and adhere to the online safety policy and to read, accept and adhere to the school's staff Acceptable Use Agreement (this is explicitly stated in employment contracts and is a condition of service).
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible. Guidance and support should be appropriate to the age of the pupils.
- Have an awareness of a range of online safety issues and how they may be experienced by the pupils in their care.

- Ensure that all pupils using technology as part of a lesson are accessing the internet on a device that is running Smoothwall, Impero or GoGuardian software, and using a network connection to the school network.
- Where internet use is pre-planned in lessons, extracurricular and extended school activities, guide pupils to sites checked as suitable for their use, and follow procedures for reporting any unsuitable material that is found in internet searches. Staff should ensure that they use "SafeSearch" when searching for content as this is enforced on pupil devices.
- Where pupils are allowed to freely search the internet during lessons, e.g. using search engines, staff should be vigilant in monitoring the content of the websites pupils visit and encourage them to use specific search terms to reduce the likelihood of coming across unsuitable material. Staff must ensure that only devices running Smoothwall, Impero or GoGuardian are used by pupils for searches.
- Be aware of the potential for cyberbullying in their lessons where malicious messages can cause hurt and distress, e.g. in collaborative shared documents in the cloud.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures as set out in the **Safeguarding and Child Protection Policy**.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

5.5. It is the responsibility of staff managing the school technical environment to:

- Provide technical support and perspective to the Designated Safeguarding Lead and to the Senior Leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures *(*including password policies and encryption*)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the Senior Leadership Team and the Online Safety Committee.
- Report any attempts to disable or circumvent filtering and monitoring to the Designated Safeguarding Lead and Senior Leadership Team, as well as to the school's technical support and Digital Strategy Lead..
- Ensure that any online inappropriate content that is not subject to filtering is added to filtering policies within 24 hours of discovery.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the Designated Safeguarding Lead, in accordance with the school's safeguarding procedures (as set out in the **Safeguarding and Child Protection Policy)**.

5.6. It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies (through surveys and the Pupil Voice).
- Read and adhere to the school's pupil Acceptable Use Agreement.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.

- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

5.7. It is the responsibility of parents and carers to:

- Read the school's pupil Acceptable Use Agreement and encourage their children to adhere to it and ensure they follow acceptable use rules at home.
- Discuss online safety issues with their children, reinforce appropriate, safe online behaviours at home and monitor their home use of ICT systems; (including mobile phones and games devices) and the internet.
- Support the TKA policy on the use of personal mobile phones and other devices in school.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's Home-School Agreement (a copy is available on the Policy Page of the school website).
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies (through surveys and online safety events organised for parents/carers).
- Use school systems, such as the Parent Portal, Show My Homework and Google Apps for education, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

6. EDUCATION AND ENGAGEMENT APPROACHES

6.1. Education and engagement with pupils

- The school has established and embedded a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in the PSHE programme, and online security and safety in the Digital Literacy programme of study, covering use both at school and home.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
    - Working with pupil Chrome Captains and Digital Leaders to amend and support online safety education within the school.

- The school will support pupils to read and understand the Acceptable Use Agreement in a way which suits their age and ability by:
    - Reviewing the Acceptable Use Agreement during a Digital Literacy lesson before pupils signify their acceptance when they access the TKA network on a fixed computer.
    - Requiring pupils to accept the Agreement every year when they log onto the TKA IT system on a fixed machine; the policy is clearly displayed on their main entry page. Their acceptance is logged.

- Displaying acceptable use posters in suitable locations around the school.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology by pupils.
- Implementing appropriate peer education approaches: number of pupils have been recruited to the national Digital Leaders programme, in which they undertake training to enable them to provide support and guidance to their peers.
- Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

6.2. Vulnerable Pupils

The Kingston Academy is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to Looked After Children, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

The Kingston Academy will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils and input will be sought from specialist staff as appropriate, including the SENCO, and the named member **of staff for** Looked After Children.

6.3. Training and engagement with staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

6.4. Awareness and engagement with parents and carers

- The Kingston Academy recognises that parents and carers have an essential role to play in enabling pupils to become safe and responsible users of the internet and associated technologies.
- The school adopts a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This includes offering specific online safety awareness training, circulating details of local online safety awareness events and highlighting online safety at other events such as parent evenings and transition events.

- Drawing their attention to the school online safety policy and expectations in newsletters, letters and on our website.
- Requesting that they read online safety information when their child joins our school
- Requiring them to read the pupil Acceptable Use Agreement and discuss its implications with their children.

7. REDUCING ONLINE RISKS AND SAFER USE OF TECHNOLOGY

- The Kingston Academy recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
  - Regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
  - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school device or other device connected to the TKA network. All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's Acceptable Use Agreement and highlighted through a variety of education and training approaches.

7.1 Classroom Use

- The Kingston Academy uses a wide range of technology. This includes access to:
  - Computers, laptops, Chromebooks and other digital devices
  - The Internet which may include search engines and relevant websites
  - Google Classroom
  - Email (web based)
  - Webcams (as part of Chromebooks)
- All school owned devices (and personal devices used in school) will be used in accordance with the school's Acceptable Use Agreements and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Pupils will be appropriately supervised when using technology, according to their ability and understanding.

7.2 Managing Internet Access

- The school will maintain a written record of users who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign an Acceptable Use Agreement before being given access to the school computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- The Kingston Academy's trustees and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The trustees and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what pupils can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the Senior Leadership Team; all changes to the filtering policy are logged and recorded.
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- The school uses educational broadband connectivity through The London Grid for Learning.
- All IT systems that use TKA connectivity are subject to filtering from an onsite appliance (Smoothwall). In addition the school uses GoGuardian (Chromebooks) and Impero (pupil facing desktop PCs) to provide additional layers of filtering. These measures together block sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list. They also flag keywords of concern.
- The school works with **GoGuardian and Smoothwall** to ensure that our filtering policy and keyword detection is continually reviewed and updated.

Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.
    - If pupils discover unsuitable sites, they will be required to turn off the monitor/screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or the Digital Learning Lead.
    - The breach will be recorded and the technical support will add identified sites to the filtering policy.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kingston Police or CEOP.

7.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
    - The provision of Smoothwall connected to the school's internet connection that monitors and logs all requests to the internet, both web pages and other traffic.

These logs are reviewed by technical staff and referrals made if necessary to the progress leaders or Digital Strategy Lead.
    - In all classroom use, teachers supervise use through visual monitoring and use of GoGuardian's teacher mode, that monitors all Chromebook tabs that are opened.
    - Where pupils use devices connected to the TKA network in an unsupervised environment, Smoothwall monitoring will log all internet traffic. In addition, GoGuardian logs all web use and uses AI to flag potential inappropriate browsing.
- The school has a clear procedure for responding to concerns identified via monitoring approaches. These are reported to the Designated Safeguarding Lead in accordance with the Safeguarding and Child Protection Policy.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 1998 and any replacement legislation and from when they are in force the General Data Protection Regulations (GDPR).
    - Full information can be found in the Data Protection Policy (a copy is available on the Policy Page of the School Website or in the Policy Folder in the Whole School Team Drive).

7.5 Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly for PCs through Sophos endpoint protection, administered centrally.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage or laptops) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be automatically checked by an anti-virus /malware scan upon use.
    - The use of TKA accounts in the Google ecosystem to store school-related information (protected by Google sign in and use of secure transmission protocols).
    - The use of two factor authentication when accessing pupil data outside the school network.
    - The use of two factor authentication by staff with admin permissions.
    - The appropriate use of user logins and passwords to access the school network.
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - Further information about technical environment safety and security can be found in the Acceptable Use Agreements

7.5.1 Password policy

- All members of staff and pupils have their own unique username and private passwords to access school systems; members of staff and pupils are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system.

- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

7.6 Managing the Safety of the School Website

- The school will ensure that information posted on our website is up to date and meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- All administrator and editor accounts for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

7.7 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to): the Data Protection Policy, Acceptable Use Agreements and the Staff Code of Conduct (copies available on the Policy Page of the School Website or in the Policy Folder in the Whole School Team Drive).

7.8 Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Acceptable Use Agreements, the Staff Code of Conduct and Communications Policy (copies available on the Policy Page of the School Website or in the Policy Folder in the Whole School Team Drive).
  - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked.
  - Electronic communication which contains confidential information relating to identifiable pupils will only be sent externally using secure and encrypted email. Staff who are required to send sensitive data should be using a USO-FX account.
  - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the Designated Safeguarding Lead if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

7.8.1 Staff

- The use of personal email addresses by staff for any official school business is not permitted.
- All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email. Emails requiring a response should not usually be sent after 20:00 on a weekday.

7.8.2 Pupils

- Pupils will use school provided email accounts for educational purposes and for all use on school premises and for school purposes.
- All pupils will agree to an Acceptable Use Agreement and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Educational use of Webcams

- The Kingston Academy recognises that the use of webcams can be a challenging activity but brings a wide range of learning benefits.
- Webcams will not be activated unless in an approved activity. Any video over IP software should not be set to auto answer.

7.9.1 Users

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will not engage in video conferencing or chat without permission, nor will they do so in an unsupervised environment.
- Videoconferencing will be supervised appropriately, according to the pupils' age and ability. A member of staff will be present at all times.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only system administrators or members of the SLT will be given access to videoconferencing administration areas or remote control pages.
- The unique login and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely in TKA Google accounts.
- If third party materials are included, the school will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-school site, staff will check that the material they are delivering is appropriate for the class.

7.10 Management of Learning Platforms

- The Kingston Academy uses Google Classroom as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, pupils and parents will have access to the LP.
- When staff and/or pupils' leave the school, their account or rights to specific school areas will be disabled.
- Pupils and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:

    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of the senior leadership team before reinstatement.
    - A pupil's parent/carer may be informed.
    - If the content is considered to be illegal, then the school will respond in line with existing safeguarding and child protection procedures.
- Pupils will require editorial approval from a member of staff for any content shared that does not require a TKA account sign in. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership team; in this instance, there may be an agreed focus or a limited time slot.

7.11 Management of Applications (apps) used to Record Pupil's Progress

- The school uses SIMS Assessment Manager and InTouch to track pupils progress and share appropriate information with parents and carers.
- The headteacher is ultimately responsible for the security of any data or images held of pupils. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation

8. SOCIAL MEDIA

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of the school community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messaging.
- All members of The Kingston Academy community are expected to engage in social media in a positive, safe and responsible manner, at all times.
- The use of social media by pupils during school hours or with school devices is not permitted.
- Inappropriate or excessive use of social media by staff during work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of The Kingston Academy community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Safeguarding policies (copies are available on the Policy Page of the School Website or in the Policy Folder in the Whole School Team Drive).

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the Staff Behaviour and Code of Conduct (available on the Policy Page

of the School Website or in the Policy Folder in the Whole School Team Drive) and within the Acceptable Use Agreement.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school and within the community. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites as strictly as they can.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of The Kingston Academy on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with the school's policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Head teacher.
    - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts or personal text messages to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head teacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead or Head teacher .

8.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications and report concerns both within school and externally.

8.4 Official Use of Social Media

The Kingston Academy's official social media channel is Twitter.

- Official school social media channels will be set up as distinct and dedicated social media sites or accounts for educational or community engagement purposes only.
    - Staff use school provided email addresses to register for and manage any official school social media channels.
    - Official social media sites are suitably protected and, where possible, run and/or link from the school website.
    - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: Anti-bullying, Data protection, Safeguarding and Child protection (copies are available on the Policy Page of the School Website or in the Policy Folder in the Whole School Team Drive).
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
    - Be professional at all times and aware that they are an ambassador for the school.
    - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
    - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
    - Ensure that they have appropriate written consent before posting images of pupils, staff or others on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
    - Inform their line manager, the Designated Safeguarding Lead and/or the Head teacher of any concerns, such as criticism, inappropriate content or contact from pupils.

9. RESPONDING TO ONLINE SAFETY INCIDENTS AND CONCERNS

- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from Children's Specialist Services.
- Where there is suspicion that illegal activity has taken place, the school will contact Children's Specialist Services or Kingston Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Kingston Police and/or Children's Specialist Services first, to ensure that potential investigations are not compromised.

9.1 Incidents outside school

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents where they are contrary to good order and discipline within the school. An investigation will take place, parents will be informed and other sanctions will be considered such as use of the behaviour support unit or even exclusion if it is deemed appropriate by the school. A referral to other agencies will also be considered if required.

9.2 Confiscation of Items

Under the Education and Inspections Act 2006 and the Education Act 2011 schools have the power to confiscate mobile phones and other personal devices, if they suspect that they are being used to

compromise the well-being and safety of others (see the Behaviour, Discipline, Exclusions Restraint and Searches Policy, a copy is available on the Policy Page of the School Website or in the Policy Folder in the Whole School Team Drive).

9.3 Concerns about Pupils' Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with local Safeguarding Children Board thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

9.4 Staff Misuse

- Any complaint about staff misuse will be referred to the Head teacher.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

9.5 Procedures for Responding to Specific Online Incidents or Concerns

All members of the school community will be made aware of the reporting procedure for online safety concerns, including:

Youth Produced Sexual Imagery or "Sexting"

- The Kingston Academy recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead in accordance with the school's Sexting policy (copy available on the Policy Page of the School Website or in the Policy Folder in the Whole School Team Drive).
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' .
- The Kingston Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Online Child Sexual Abuse and Exploitation

- The Kingston Academy ensures that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The Kingston Academy recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

- The 'Click CEOP' report button is visible and available to pupils and other members of the school community on the school website.

Dealing with Online Child Sexual Abuse and Exploitation

- If the school is made aware of incident involving online sexual abuse of a child, the school will:
  - Act in accordance with the school's Safeguarding and Child Protection policy.
  - Immediately notify the Designated Safeguarding Lead.
  - Store any devices involved securely.
  - Immediately inform Kingston police via 101 (or 999 if a child is at immediate risk)
  - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
  - Inform parents/carers about the incident and how it is being managed.
  - Make a referral to Children's Specialist Services (if required/ appropriate).
  - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
  - Review the handling of any incidents to ensure that best practice is implemented; the Senior Leadership Team will review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : www.ceop.police.uk/safety-centre/
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Children's Specialist Services and/or Kingston Police.
- If pupils at other schools are believed to have been targeted, the school will seek support from Kingston Police and/or Children's Specialist Services first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- The Kingston Academy will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Kingston Police and/or Children's Specialist Services.
- If made aware of IIOC, the school will:
  - Act in accordance with the school's Safeguarding and Child Protection policy and the relevant local Safeguarding Child Boards procedures.
  - Immediately notify the school Designated Safeguard Lead.
  - Store any devices involved securely.

- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kingston police or the LADO.

- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on school devices, the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Specialist Services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police.
  - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
  - Ensure that the head teacher is informed.
  - Inform the Local Authority Designated Officer (LADO) in accordance with the school's managing allegations policy.
  - Quarantine any devices until police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at The Kingston Academy. Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy (copy available on the Policy Page of the School Website or in the Policy Folder in the Whole School Team Drive)..

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at The Kingston Academy and will be responded to in line with existing school policies, including Anti-bullying and Behaviour (copies available on the Policy Page of the School Website or in the Policy Folder in the Whole School Team Drive).
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through Children's Specialist Services and/or Kingston Police.

Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Safeguarding and Child Protection Policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Head teacher will be informed immediately and action will be taken in line with the Safeguarding and Child Protection and Allegations policies (copies available on the Policy Page of the School Website or in the Policy Folder in the Whole School Team Drive).

10. USEFUL LINKS

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

This policy will be reviewed annually in accordance with section 3 above.
Next review due: March 2019

Date: 12 March 2018
Signed:

Sue Conder, Chair Pupil Welfare and Community Committee
Sophie Cavanagh, Head teacher