



Online Safety Policy

CONFIDENT · INDEPENDENT · FORWARD -THINKING

ADOPTION AND AMENDMENTS TO ONLINE SAFETY POLICY

Written February 2019

Section	Governors' Meeting or Committee	Page and Year of Minute
Whole document	LGB 14 th February 2019	14 th February page 5/5
	Next Review: 2019/2020	

Aims and Values of the Policy

Kents Hill Park School is an all-through school providing both Primary and Secondary education for ages 4 through to 16. The school aims to teach a rich and balanced curriculum ensuring that pupils can meet their full potential.

Online Safety encompasses internet technologies, but also electronic communication platforms such as mobile phones, tablets and wireless technology. It highlights the need to educate pupils, young adults and staff about the benefits, risks and responsibilities of using information technology. The Online Safety policy also highlights safeguarding issues and raises awareness to enable users to control their online experiences, especially given that the internet is an unmanaged, open channel of communication. The focus of the policy is aimed primarily towards Online Safety within school and it is worth noting that for some incidences outside of school, policing will be difficult.

Policy Statement

For clarity, the Online Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, members of the governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents.

Safeguarding is a serious matter; at Kents Hill Park School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as Online Safety is an area that is constantly evolving and as such this policy will be reviewed on at least an annual basis.

The purpose of this policy is twofold:

1. To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
2. To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any possibility/foreseeability of harm to the pupil or liability to the school.

This policy is available for anybody to read on the Kents Hill Park School website; upon review all members of staff will sign as read and understood both the Online Safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Pupils Acceptable Use Policy will need to be agreed to when a pupil starts at Kents Hill Park.

Headteacher Name: Mr James Pilgrim

Chair of Governors:

Review Date: January 2019

Next Review: 2019/2020

Policy Governance (Roles & Responsibilities)

Local Governing Body

The governing body is accountable for ensuring that Kents Hill Park School has effective policies and procedures in place; as such they will:

1. Review this policy and receive a report at least annually to ensure that the policy is up to date, covers all aspects of technology use within the school, ensure Online Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
2. Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will:
 - Receive regular updates from the Headteacher and/or Online Safety Officer in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for Online Safety within the school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Officer (or more than one), as indicated below.

The Headteacher will ensure that:

1. Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
2. The designated Online Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
3. All Online Safety incidents are recorded and dealt with promptly and appropriately.

Online Safety Officer

The Online Safety Officer will:

1. Keep up to date with the latest risks to children and young people whilst using technology; familiarize themselves with the latest research and available resources for school and home use;
2. Review this policy regularly and bring any concerns to the attention of the Headteacher;
3. Advise the Headteacher and governing body on all Online Safety matters;

4. Engage with parents and the school community on Online Safety matters at school and/or at home;
5. Liaise with the local authority, IT technical support and other agencies as required;
6. Ensure staff know what to report on MyConcern and ensure the appropriate audit trail;
7. Ensure any technical Online Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support;
8. Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident;
9. To facilitate training and advice for all staff.

Designated Safeguarding Lead (DSL)/Pastoral Team

The Designated Safeguarding Lead/Pastoral Team will:

1. Take day to day responsibility for Online Safety issues and has a role in establishing and reviewing the school Online Safety policies/documents;
2. Liaise with the Local Authority and relevant agencies;
3. Be regularly updated in Online Safety issues and legislation, and be aware of the potential for serious child protection issues arising from:
 - a) Sharing of personal data;
 - b) Access to illegal/inappropriate materials;
 - c) Inappropriate on-line contact with adults/strangers;
 - d) Potential or actual incidents of grooming;
 - e) Cyber-bullying and use of social media.

ICT Technical Support Staff

ICT technical support staff are responsible for ensuring that:

1. The IT technical infrastructure is secure; this will include at a minimum:
 - a) Anti-virus that is fit-for-purpose, up to date and applied to all capable devices;
 - b) Windows (or other operating system) updates are regularly implemented and devices updated as appropriate;
 - c) Any Online Safety technical solutions, such as Internet filtering, are operating correctly;
 - d) Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Online Safety officer and Headteacher;
 - e) Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 6 characters consisting of upper and lower case letters and at least one number and an enforced change will take place every 3 months;
 - f) The IT System Administrator password is to be changed on a monthly (30 day) basis;
 - g) The staff do not misuse ICT equipment and are fully aware of their duty of care.

All Staff

Staff are to ensure that:

1. All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher;
2. Any Online Safety incident is reported to the Online Safety Officer/DSL /Pastoral Team (and recorded on MyConcern), or in his/her absence to the Headteacher. If you are unsure, the matter is to be raised with the Online Safety Officer or the Headteacher to make a decision;
3. Online Safety training is attended during every academic year;
4. They adhere to the Staff Code of Conduct Policy.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the pupil Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour, Anti-Bullying and/or Child Protection and Safeguarding policy.

Online Safety is embedded in the curriculum at Kents Hill Park; pupils will be given the appropriate advice and guidance by staff. Similarly all pupils will be made fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents/Carers play the principal role in the development of their children; as such the school will endeavor to provide parents/carers with relevant information to help them to develop the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings and school newsletters/communications we will endeavour to keep parents/carers up to date with new and emerging Online Safety risks, and will involve parents/carers in strategies to ensure that pupils are empowered to keep themselves e-safe.

Parents/Carers must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents/carers will need to be aware of and agree to the pupil Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

Kents Hill Park School uses a range of devices including PC's, laptops, tablets and digital video recorders. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use appropriate software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Online Safety Officer and IT Support are responsible

for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use appropriate software that seeks to prevent any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. Kents Hill Park currently uses Microsoft 365 email account. Emails are kept indefinitely, allowing for full conversation history years down the line.

Passwords – all staff and pupils are unable to access any device without a unique username and password. With effect from September 2015, staff will be required to change their passwords on a 3 monthly basis or if there has been a compromise, whichever is sooner.

Anti-Virus – All capable devices have anti-virus software. This software is updated daily for new virus definitions. IT Support are responsible for ensuring this task is carried out, and report to the Headteacher if there are any concerns.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted to staff upon signing the Staff Acceptable Use Policy; to pupils upon them and parents/carers signing the Acceptable Use Policy. The Behaviour, Anti-Bullying and/or Child Protection and Safeguarding policies may be applied to any misuse of the internet inside or outside of school.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Pupils are permitted to use the school email system, and as such will be given their own email address. The email address will be made up of their initial and surname, e.g. jsmith@KentsHillPark.school.

The Behaviour, Anti-Bullying and/or Child Protection and Safeguarding policies may be applied to any misuse of the email inside or outside of school.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photography Policy.

Social Networking – there are many social networking services available; Kents Hill Park School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents/carers and the wider school community. The following social media services are permitted for use within Kents Hill Park School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the Online Safety Officer who will advise the Headteacher for a decision to be made. Reference should also be made to the Staff Code of Conduct Policy.

1. Blogging – used by staff and pupils in school.
2. Twitter – used by the school as a broadcast service (see below).
3. Facebook – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be “followed” or “friended” on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

1. SIMS must be consulted before any image or video of any child is uploaded to make sure permission has been given (via the school photography policy).
2. There is to be no identification of pupils using first name and surname; first name only is to be used.
3. Where services are “comment enabled”, comments are to be set to “moderated”.
4. All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school’s attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any Online Safety incident is to be brought to the immediate attention of the Online Safety Officer/DSL/Pastoral Team, or in his/her absence the Headteacher. The Online Safety Officer/Designated Child Protection Lead/Pastoral Team will assist in taking the appropriate action to deal with the incident using the relevant policy (Behaviour Management, Anti-Bullying and Child Protection and Safeguarding) and recording the incident on MyConcern.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Kents Hill Park School will have an annual programme of training which is suitable to the audience. Should any member of staff feel they have had insufficient training generally or in any particular area this must be brought to the attention of the Online Safety Officer or Headteacher for further CPD.

Online Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil’s learning. Kents Hill Park School has a clear, progressive Online Safety education programme as part of the Computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

1. To STOP and THINK before they CLICK;
2. To develop a range of strategies to evaluate and verify information before accepting its accuracy;

3. To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
4. To know how to narrow down or refine a search;
5. To understand how search engines work and to understand that this affects the results they see at the top of the listings (for older pupils);
6. To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
7. To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
8. To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
9. To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
10. To understand why they must not post pictures or videos of others without their permission;
11. To know not to download any files – such as music files - without permission;
12. To have strategies for dealing with receipt of inappropriate materials;
13. To understand why and how some people will 'groom' young people for sexual reasons (for older pupils);
14. To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying;
15. To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

Kents Hill Park School
January 2019

Staff, Governor and Visitor Acceptable ICT Use Agreement

ICT and the related technologies such as email, the Internet and mobile devices 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 ICT Network Manager.

1. I will only use the school's email / Internet / VLE and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
2. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities and not use this password for any other non-school related systems.
3. I will ensure that my password is suitably complex (i.e. at least 6 characters consisting of upper and lower case letters and at least one number) and only enter it into secure systems provided by the school.
4. I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
5. I will only use the approved email system for any communications with pupils, parents and other school related activities; this excludes social networking, online purchases, online banking, online auction sites and sales/offers notifications. I will not give out my own personal details, such as mobile phone number, personal email address or social networking address to pupils.
6. I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body and with appropriate levels of security in place.
7. I will not install any hardware or software on school equipment without the prior permission of the ICT Network Manager.
8. I will report any accidental access to inappropriate materials immediately to the ICT Network Manager.
9. I will not browse, download, upload, distribute or playback any material that could be considered offensive, illegal or discriminatory.
10. Images of pupils and/or staff should only be taken on authorised equipment, 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/carers, member of staff or Headteacher in line with data security policy.
11. 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.
12. I will respect copyright and intellectual property rights.
13. 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).

14. I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Signature Date

Full Name (Printed)

Acceptable ICT Use Agreement for ICT Support Staff

This policy is to help ensure that all ICT Support Staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All ICT Support 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 SLT.

1. I will only use the school's email / Internet / VLE and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
2. I will agree not to use school systems passwords for any other non-school related systems.
3. I will ensure that my password is suitably complex (i.e. at least 6 characters consisting of capital letters, numbers and special characters are included) and only enter it into secure systems provided by the school.
4. I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
5. I will only use the approved email system for any communications with pupils, parents and other school related activities; this excludes social networking, online purchases, online banking, online auction sites and sales/offers notifications. I will not give out my own personal details, such as mobile phone number, personal email address or social networking address to pupils.
6. I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body and with appropriate levels of security in place.
7. I will only install any hardware or software on school equipment in accordance with my professional role.
8. I will report any observed access to inappropriate materials by pupils and visitors immediately as required by the school's policies.
9. I will not browse, download, upload, distribute or playback any material that could be considered offensive, illegal or discriminatory unless required by my professional role.

10. Images of pupils and/or staff should only be taken on authorised equipment, 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/carers, member of staff or Headteacher in line with data security policy.
11. 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.
12. I will respect copyright and intellectual property rights.
13. 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).
14. I will support and promote the school's Online Safety policy and help pupils, staff and visitors to be safe and responsible in their use of ICT and related technologies.
15. I will only view staff emails or files under the following circumstances:
 - When requested by SLT;
 - When requested by a member of staff's line manager;
 - If emails or files are left open when I am attending a support call.
16. Any emails caught in anti-spam measures will be vetted by the ICT Support Staff as directed by the ICT Network Manager.
17. When reviewing network logs or monitoring the network, there is a strong likelihood that we will become aware of the websites visited by the all of the users of the school's system.
18. Any information available in an electronic format on or connected to the school system will be accessible by all of the ICT Support Staff due to the nature of how computer systems work. However, I will access these only if required for my day-to-day duties.
19. I will routinely scan the school network and delete/uninstall any illegal files or applications found and report as required by school policies or the law. A list of what scans the ICT Support Department perform can be made available to SLT.
20. I will routinely scan the pupils' user areas for any non-school related files or applications and delete/uninstall them and report as required by school policies or the law. A list of what scans the ICT Support Department perform can be made available to SLT.
21. Any information seen or heard whilst performing my duties will remain confidential unless requested by SLT, school policies or required by law enforcement agencies.

User Signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school. I understand that failure to abide by this agreement will result in disciplinary action.

Signature Date

Full Name (Printed)



☎ 01908 533290

✉ enquiries@kentshillpark.school

🌐 www.kentshillpark.school

Kents Hill Park School is part of the Kingsbridge Educational Trust, a charitable company limited by guarantee and registered in England and Wales with company number 09144847. The registered office is at Oakgrove School, Venturer Gate, Middleton, Milton Keynes, MK10 9JQ. Telephone number: 01908 545300