KINGHAM HILL SCHOOL

E-Safety Policy

1. Scope

- Kingham Hill School is committed to promoting and safeguarding the welfare of all pupils and an effective online safety strategy is paramount to this.
- The aims of the School's online safety strategy are threefold:
    - To protect the whole School community from illegal, inappropriate and harmful content or contact
    - To educate the whole School community about their access to and use of technology
    - To establish effective mechanisms to identify, intervene and escalate incidents where appropriate.
- In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications Technology (collectively referred to in this policy as **Technology**).
- This policy applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's Technology whether on or off School premises, or otherwise use Technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.
- The following policies, procedures and resource materials are also relevant to the School's online safety practices:
    - KHS ICT Strategy and Usage Policy
    - IT Acceptable Use Policy (Pupils, Parents and Visitors)
    - IT Acceptable Use Policy (Staff)
    - Safeguarding and Child Protection Policy and Procedures
    - Anti-bullying policy
    - Risk Assessment Policy and Guidance
    - Staff Handbook
    - Whistleblowing Policy
    - Data Protection Policy

- Remote Working and Bring Your Own Device to Work Policy
- Data Tracking and the Retention of Information Policy
- Privacy Notices for Staff, Pupils and Parents
- PHSEE Handbook
- Capture and Use of Photographic and Video Images of Pupils Policy.

- These policies procedures and resource materials are available to staff on the School's intranet and hard copies are available on request.

2. Roles and responsibilities

- **The Governing Body**

  - The Governing Body as proprietor has overall responsibility for safeguarding arrangements within the School, including the School's approach to online safety and the use of Technology within the School
  - The Governing Body is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Governing Body's response to this duty
  - The Nominated Safeguarding Governor is Ruth Reavley. The Nominated Safeguarding Governor is the senior board level lead with leadership responsibility for the School's safeguarding arrangements, including the School's online safety procedures, on behalf of the Governing Body. This role includes:
    - Ensuring an e-safety Policy is in place, which is reviewed annually and available to all stakeholders
    - Ensuring there is an e-safety Co-ordinator who has received appropriate CEOP training (Child Exploitation and Online Protection)
    - Ensuring procedures for the safe use of ICT and the Internet are in place and adhered to.
  - The Governing Body will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies in meeting the aims set out in section 1 above.

- **Head**

  - The Head has overall executive responsibility for the safety and welfare of members of the School community
  - The Head, together with the DSL, Second Deputy and ICT Manager, is responsible for reviewing the weekly filter access requests from staff and pupils and formally approving the 'white listing' of any sites

- The Head is responsible for ensuring that training and induction in e-Safety best practice and data protection is provided to all staff and pupils.

- **Bursar**

  - The Bursar is responsible for monitoring, in conjunction with the DSL, the daily Smoothwall filtering report relating to staff and visitor network usage and actioning issues as appropriate

  - The Bursar is responsible for ensuring all staff have signed the School IT Acceptable Use Policy (Staff)

  - In the absence of the Head, DSL and Second Deputy, the Bursar can approve the permanent 'white listing' of websites.

- **Second Deputy**

  - The Second Deputy is responsible for monitoring, in conjunction with the DSL, the daily Smoothwall filtering report relating to pupil network usage and auctioning issues as appropriate

  - The Second Deputy, together with the Head, DSL and ICT Manager, is responsible for reviewing the weekly filter access requests from staff and pupils and formally approving the 'white listing' of any sites

  - The Second Deputy is responsible for ensuring all pupils have signed the School IT Acceptable Use Policy (Pupils, Parents and Visitors).

- **Designated Safeguarding Lead (DSL)**

  - The Designated Safeguarding Lead (DSL) is the senior member of staff from the School's management team with lead responsibility for safeguarding and child protection. The responsibility of the DSL includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding and Child Protection Policy and Procedures

  - The Designated Safeguarding Lead fulfils the role of the e-Safety Coordinator and will work with the ICT Manager (see below) in monitoring Technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

    - As e-Safety Coordinator, the DSL is a member of the ICT and E-Safety Committee, which is chaired by the Second Deputy.

  - The Designated Safeguarding Lead (or a member of their team) will monitor the Technology Incident Log maintained by the ICT Manager

  - The Designated Safeguarding Lead will regularly update other members of the School's Senior Management Team on the operation of the School's safeguarding arrangements, including online safety practices

- The DSL is responsible for monitoring, in conjunction with the DSL and Bursar, the daily Smoothwall filtering report relating to pupil and staff network usage and actioning issues as appropriate

- The DSL, together with the Head, Second Deputy and ICT Manager, is responsible for reviewing the weekly filter access requests from staff and pupils and formally approving the 'white listing' of any sites

- The DSL will include an e-Safety update to the Governors as part of the annual safeguarding report

- The DSL is Rob Jones.

- **ICT Manager**

  - The ICT Manager, together with their team, is responsible for the effective operation of the School's filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network

  - The ICT Manager is responsible for ensuring that:

    - The School's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack

    - The user may only use the School's Technology if they are properly authenticated and authorised

    - The School has an effective filtering policy in place and that it is applied and updated on a regular basis

    - The risks of pupils and staff circumventing the safeguards put in place by the School are minimised

    - The use of the School's Technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation

    - Monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

  - The School utilises anti-virus software to safeguard the School network and hardware from malware, including viruses, computer worms, and Trojan horses. Antivirus software may also remove or prevent spyware and adware, along with other forms of malicious programs. In addition the School uses firewall and web content filtering software called Smoothwall and Google SafeSearch to filter and block more potentially harmful material

  - The ICT Manager will report regularly to the Senior Management Team on the operation of the School's Technology. This will comprise meetings with the Bursar regarding operational and strategic level ICT matters and meeting with the Head and DSL regarding filtering and E-Safety.

If the ICT Manager has concerns about the functionality, effectiveness, suitability or use of Technology within the School, including the monitoring and filtering systems in place, he will escalate those concerns promptly to the appropriate members(s) of the School's Senior Management Team

- The ICT Manager has the authority to temporarily 'white list' websites for the immediate benefit of teaching and learning or the efficient running of the School. Permanent approval is granted by the Head, DSL and Second Deputy at the weekly safeguarding meeting. During the holidays, the Bursar can grant permanent approval

- The ICT Manager is responsible for maintaining the Technology Incident Log (a central record of all serious incidents involving the use of Technology), and bringing any matters of safeguarding concern to the attention of the DSL in accordance with the School's Safeguarding and Child Protection Policy and Procedures.

- **All staff**

  - The School staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with the pupils

  - Staff are expected to adhere, so far as applicable, to each of the policies referenced in section 1 above

  - Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding and Child Protection Policy and Procedures.

  - Requests to access websites blocked by the filtering system, may be made to the ICT Manager using the appropriate Google Form

  - Further information regarding staff usage of the internet is contained in the KHS Staff Handbook.

- **Parents**

  - The role of parents in ensuring that pupils understand how to stay safe when using Technology is crucial. The School expects parents to promote safe practice when using Technology and to:

    - Support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures

    - Talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour

    - Encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

- If parents have any concerns or require any information about online safety, they should contact the DSL.

3. Education and training

- **Pupils**
  - The safe use of Technology is integral to the School's ICT curriculum via chapel assemblies and PHSE. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices (see the School's Curriculum Policy)
  - The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/ pastoral activities, teaching pupils:
    - About the risks associated with using the Technology and how to protect themselves and their peers from potential risks
    - To be critically aware of content they access online and guided to validate accuracy of information
    - How to recognise suspicious, bullying or extremist behaviour
    - The definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect
    - The consequences of negative online behaviour
    - How to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.
  - The safe use of Technology aspects of the curriculum are reviewed on a regular basis to ensure their relevance
  - The School's acceptable use policy for pupils sets out the School rules about the use of Technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using Technology. Pupils are reminded of the importance of this policy on a regular basis.
  - Useful online safety resources for pupils:
    - http://www.thinkuknow.co.uk/
    - http://www.childnet.com/young-people
    - https://www.saferinternet.org.uk/advice-centre/young-people
    - https://www.disrespectnobody.co.uk/
    - http://www.safetynetkids.org.uk/

- **Staff**
    - The School provides training on the safe use of Technology to staff so that they are aware of how to protect pupils and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur
    - Induction training for new staff includes training on the School's online safety strategy including this policy, the Staff Code of Conduct, Social Media Policy and the IT Acceptable Use Policy (Staff). Ongoing staff development training includes training on Technology safety together with specific safeguarding issues including sexting, cyberbullying and radicalisation
    - Staff also receive data protection training on induction and at regular intervals afterwards
    - The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding
    - Useful online safety resources for staff:
        - http://swgfl.org.uk/products-services/esafety
        - https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals
        - http://www.childnet.com/teachers-and-professionals
        - https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
        - https://www.thinkuknow.co.uk/teachers/
        - http://educateagainsthate.com/
        - DfE's Advice for head teachers and school staff on cyberbullying
        - DfE's Advice on the use of social media for online radicalisation
        - UKCCIS Sexting in schools and colleges
        - UKCCIS Online safety in schools and colleges: Questions from the Governing Board
        - College of Policing Briefing Note: Police action in response to youth produced sexual imagery
        - Professionals Online Safety Helpline: helpline@saferinternet.org.uk, 0344 381 4772
    - The Oxfordshire Safeguarding Children Board has recommended the following guidance for parents on radicalisation: http://educateagainsthate.com/.

- **Parents**

    - The School informs, communicates with and educates parents in the safe use of Technology via email updates from the DSL, the e-Safety section of the School website and E-safety briefings for parents

    - Parents are encouraged to read the acceptable use policy for pupils with their son/daughter to ensure that it is fully understood

    - Useful online safety resources for parents:

        - https://www.saferinternet.org.uk/advice-centre/parents-and-carers
        - http://www.childnet.com/parents-and-carers
        - https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
        - https://www.thinkuknow.co.uk/parents/
        - http://parentinfo.org/
        - http://parentzone.org.uk/
        - https://www.net-aware.org.uk
        - https://www.internetmatters.org/
        - DfE's Advice for parents and carers on cyberbullying

4. Access to the School's Technology

- The School provides internet, intranet, and in the case of staff with a business need, social media access and an email system to pupils and staff as well as other Technology. Pupils and staff must comply with the respective acceptable use policy when using School Technology. All such use is monitored by the ICT team.

- Internet and Social Media access for pupils, staff and visitors is controlled in accordance with the KHS SmoothWall Filter Settings document, which is a live Google document owned by the ICT Manager.

- Pupils and staff require individual user names and passwords to access the School's internet, intranet and email system which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their user names or passwords must report it to the ICT team immediately.

- No laptop or other mobile electronic device may be connected to the School network without the consent of the ICT Manager. All devices are controlled by MAC address and cannot join the network, with the exception of the guest network, without the provision of a MAC address. All personal devices should have up-to-date anti-virus software installed. The use of any device connected to the School's network will be logged and monitored by the ICT team.

- The School has a separate Wi-Fi connection available for use by visitors to the School.

A unique password valid for 24 hours, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the ICT team. Passwords are available from Reception, KHL and the ICT Manager.

- **Use of mobile electronic devices**

    - The School has appropriate filtering and monitoring systems in place to protect pupils using the Internet (including email text messaging and social media sites) when connected to the School's network. Mobile devices equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet. Since the School cannot restrict the content available via 3G and 4G, all personal devices are locked away during core School hours and access is granted outside the School day in accordance with the KHS SmoothWall Filter Settings document and the KHS ICT Strategy and Usage Policy. In certain circumstances, a pupil may be given permission to use their own mobile device during the School day but permission to do so must be sought from their Houseparent

    - The School rules about the use of mobile electronic devices are set out in the IT Acceptable Use Policy (Pupils, Parents and Visitors)

    - The use of mobile electronic devices by staff is covered in the KHS Staff Handbook, IT Acceptable Use Policy (Staff), Data Protection Policy for Staff and Remote Working and Bring Your Own Device to Work Policy. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency

    - The School's policies apply to the use of Technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

5. Procedures for dealing with incidents of misuse

- Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding, whistleblowing and disciplinary policies and procedures.

- **Misuse by pupils**

    - Anyone who has any concern about the misuse of Technology by pupils should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the anti-bullying policy where there is an allegation of cyberbullying

    - Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding and Child Protection Policy and Procedures).

- **Misuse by staff**

    - Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures

    - If anyone has a safeguarding-related concern, they should be report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding and Child Protection Policy and Procedures.

- **Misuse by any user**

    - Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the ICT Manager, DSL, Bursar or the Head

    - The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police

    - If the School considers that any person is vulnerable to radicalisation the School will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

6. Monitoring and Review

- All serious incidents involving the use of Technology will be logged centrally in the Technology Incident Log by the ICT Manager, Second Deputy, DSL or DDSL.

- The DSL has responsibility for the implementation and review of this policy. The DSL will consider the views of pupils and parents together with the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures and to consider whether existing security and online safety practices within the School are adequate.

- Consideration of the effectiveness of the School's online safety procedures and the education of pupils about keeping safe online will be included in the Governors' annual review of safeguarding.

Nick Seward and Catriona Thompson

Last reviewed: August 2018

To be reviewed: April 2019