

Online Safety Policy

Policy Number:	N148
Policy Owner:	Head of Curriculum ICT & Network Manager
Governing Body Responsibility:	Welfare Committee
Version:	3.0
Date:	January 2022

Policy to be reviewed on or before January 2024



Kesteven and Grantham Girls' School

Contents

1. CREATING AN ONLINE SAFETY ETHOS.....	4
1.1 AIMS	4
1.2 WRITING AND REVIEWING THE ONLINE SAFETY POLICY.....	4
1.3 KEY RESPONSIBILITIES FOR THE COMMUNITY.....	5
2. ONLINE COMMUNICATION AND SAFER USE OF TECHNOLOGY	7
2.1 MANAGING THE KGGS WEBSITE	7
2.2 PUBLISHING IMAGES AND VIDEOS ONLINE	8
2.3 MANAGING EMAIL	8
2.4 APPROPRIATE AND SAFE CLASSROOM USE OF THE INTERNET AND ANY ASSOCIATED DEVICES.....	8
2.5 MANAGEMENT OF SCHOOL LEARNING PLATFORMS/PORTALS/GATEWAYS	9
3. SOCIAL MEDIA POLICY	9
3.1. GENERAL SOCIAL MEDIA USE	9
3.2 OFFICIAL USE OF SOCIAL MEDIA	10
3.3 STAFF PERSONAL USE OF SOCIAL MEDIA	11
3.4 STAFF OFFICIAL USE OF SOCIAL MEDIA	13
3.5 PUPILS USE OF SOCIAL MEDIA.....	13
4. USE OF PERSONAL DEVICES AND MOBILE PHONES	14
4.1 RATIONALE REGARDING PERSONAL DEVICES AND MOBILE PHONES	14
4.2 EXPECTATIONS FOR SAFE USE OF PERSONAL DEVICES AND MOBILE PHONES	14
4.3 PUPILS USE OF PERSONAL DEVICES AND MOBILE PHONES	15
4.4 STAFF USE OF PERSONAL DEVICES AND MOBILE PHONES.....	16
4.5 VISITORS USE OF PERSONAL DEVICES AND MOBILE PHONES.....	17
5. POLICY DECISIONS	17
5.1. REDUCING ONLINE RISKS	17
5.2 AUTHORISING INTERNET ACCESS	18
6. ENGAGEMENT APPROACHES.....	18
6.1 ENGAGEMENT AND EDUCATION OF STUDENTS	18
6.2 ENGAGEMENT AND EDUCATION OF STUDENTS CONSIDERED TO BE VULNERABLE.....	18
6.3 ENGAGEMENT AND EDUCATION OF STAFF	19
6.4 ENGAGEMENT AND EDUCATION OF PARENTS AND CARERS.....	19
7. MANAGING INFORMATION SYSTEMS.....	20
7.1 MANAGING PERSONAL DATA ONLINE.....	20
7.2 SECURITY AND MANAGEMENT OF INFORMATION SYSTEMS	20
7.3 FILTERING AND MONITORING	21
8. RESPONDING TO ONLINE INCIDENTS AND SAFEGUARDING CONCERNS.....	22
APPENDIX A.....	23
9. PROCEDURES FOR RESPONDING TO SPECIFIC ONLINE INCIDENTS OR CONCERNS	23
9.1 RESPONDING TO CONCERNS REGARDING YOUTH PRODUCED SEXUAL IMAGERY OR “SEXTING”	23
9.2. RESPONDING TO CONCERNS REGARDING ONLINE CHILD SEXUAL ABUSE AND EXPLOITATION.....	24
9.3. RESPONDING TO CONCERNS REGARDING INDECENT IMAGES OF CHILDREN (IIOC)	26
9.4. RESPONDING TO CONCERNS REGARDING RADICALISATION AND EXTREMISM ONLINE	27
9.5. RESPONDING TO CONCERNS REGARDING CYBERBULLYING	27
9.6 RESPONDING TO CONCERNS REGARDING ONLINE HATE	28

APPENDIX E	29
ONLINE SAFETY (E-SAFETY) CONTACTS AND REFERENCES	29
NATIONAL LINKS AND RESOURCES	29
CONFIGURATION HISTORY	30

1. Creating an Online Safety Ethos

1.1 Aims

1. Kesteven and Grantham Girls' School (KGGs) believes that online safety (e-Safety) is an essential element of safeguarding children and adults. Students must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online and report concerns without worry.
2. The purpose of the KGGs online safety policy is to:
 - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that KGGs is a safe and secure environment.
 - Safeguard and protect all members of the KGGs community online.
 - Raise awareness with all members of the KGGs community regarding the potential risks as well as benefits of technology.
 - To enable all staff to work safely and responsibly, 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 community, both staff and students.
3. This policy applies to all staff including the governing body, teachers and support staff (collectively referred to as 'staff' in this policy) as well as students.
4. This policy applies to all access to the internet and use of information communication devices, including personal devices, or where students, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
5. This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, mobile telephone and electronic devices, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE).

1.2 Writing and reviewing the online safety policy

The Designated Safeguarding Lead (DSL) is Tracey Doig

The Deputy Designated Safeguarding Leads (DSL) are Sally Macpherson and Amanda Hubbard

The Online safety (e-Safety) lead for KGGs is Matthew Dovey

The Online safety (e-Safety) lead for the Governing Body is Nick Flanagan

The Curriculum Co-Ordinator for e-safety is Piers Mayfield

The policy will be reviewed every 2 years.

1.3 Key responsibilities for the community

1.3.1 The key responsibilities of the management and leadership team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL), the Curriculum Co-ordinator and E-safety lead by ensuring they have sufficient time and resources to fulfil their online safety roles and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect students from inappropriate content which meet the needs of the school community, whilst ensuring they have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school's network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Maintaining a record of online safety concerns/incidents in line with the existing child protection procedures and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.3.3 The key responsibilities for all members of staff are:

- Reading the school Acceptable Use Policy (AUPs) and adhering to the points.
- Being aware that they can contribute to the development of the online safety policy.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the students in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever appropriate, including discrete lessons delivered via the Computing and PSHE curriculum.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Ensuring that all communication between staff and members of the school community on school business takes place via official approved communication channels (such as an official setting provided email address or phone numbers) and not via other methods, such as private email or social media accounts

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the SLT.
- Ensuring that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering procedure is applied and updated on a regular basis.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.

1.3.5 The key responsibilities of students are:

- Reading the school's Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.

- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents and carers are:

- Reading the school's Acceptable Use Policy summary and encouraging their daughters to adhere to the rules.
- Discussing online safety issues with their daughters, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Seeking help and support from appropriate agencies, if they or their child encounters online problems or concerns.

2. Online Communication and Safer Use of Technology

2.1 Managing the KGGS website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school/setting address, email and telephone number. Staff or pupils' personal information *will not* be published.
- SLT will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
 - Pupils work will only be published with their permission or that of their parents/carers.
 - The administrator account for the school website will be safeguarded with an appropriately strong password.
 - The school will post information about safeguarding, including online safety, on the school website for members of the community.

2.2 Publishing images and videos online

- The school will ensure that all use of images and videos take place in accordance with other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, Image policy, use of personal devices and mobile phones etc.

2.3 Managing email

- All members of staff are provided with a specific KGS email address to use for any official communication.
- The use of personal email addresses by staff for any official KGS business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure email.
- Emails should be accessed in a secure environment where confidentiality can be ensured.
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- Official email sent to external organisations that represent KGS should be written carefully in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Appropriate and safe classroom use of the internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils and access levels will be appropriate to their age and ability
- All school owned devices will be used in accordance with the school Acceptable Use Policy 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.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- The school will ensure web searches are filtered in the same way as other material, both in blocking inappropriate results from innocent queries and in blocking inappropriate queries outright. Where available search engines should be forced into Safe Search mode (or equivalent).
- The users will ensure that the use of Internet-derived materials complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

2.5 Management of school learning platforms/portals/gateways

- Staff should review their subject areas in the shared file areas (accessible via External File Access) and on any online curriculum resources they subscribe to, in particular message and communication tools and publishing facilities.
- Only members of the current pupil, parent/carers and staff community will have access to the External File Access and any online curriculum resources the school subscribes to.
- All users will be mindful of copyright issues and will only upload appropriate content onto the External File Access and any online curriculum resources the school subscribes to.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled.
- Any concerns about content on the external file system will be recorded and dealt with in the following ways:
 - a) The material will be removed by the site administrator and the user will be notified.
 - b) Access to the External File Access system for the user may be suspended and reviewed later. Relevant parties will be informed.

3. Social Media Policy

3.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the KGGS community and exist to safeguard both the school and the wider community, on and offline.
- All members of the KGGS community will be encouraged to use social media in a positive, safe and responsible manner **at all times**.
- Information about safe and responsible use of social media will be communicated as appropriately, clearly and regularly to all members of the KGGS community.

- It is an individual's responsibility to monitor and ensure that their private settings are set appropriately and that they are regularly reviewed.
- All members of the KGGs community are strongly advised to refrain from publishing specific and detailed private thoughts, concerns, pictures or messages on any social media services in a publicly accessible arena especially content that may be considered threatening, hurtful or defamatory to others.
- The school will restrict pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems.
- The use of social networking applications during school hours for personal use **is not** permitted, except:
 - Staff may use the standalone computer in the staffroom, which has unfiltered internet access, for reasonable social media use during non-contact periods.
 - Students may use social media under the explicit supervision of pastoral and technical staff for the purpose of retrieving evidence (e.g. of cyberbullying) or retrieving work.
- Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the KGGs community on social media sites should be reported to SLT and will be managed in accordance with policies.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with relevant policies.

3.2 Official use of social media

- KGGs official social media channels are:
 - @KGGSchool (Twitter)--main school account, active
 - Run by Alison Evershed, sometimes by Matt Dovey
 - @KGGsPE (Twitter)--for fixtures, results etc., active
 - Run by PE department (all have access)
 - @KGGsHistory--curriculum account, inactive
 - Formerly Helen Robinson, currently unclaimed
 - @KGGsGeography--curriculum account, inactive
 - Lyndon Cowlard
 - @KGGsICT--curriculum account, currently inactive
 - Piers Mayfield
 - *DT: Product Design AS & A2* (YouTube)--curriculum account, active, used for uploading coursework videos and gathering feedback for part of assessment

- Run by Pav Mears-Sagoo with assistance from Matt Dovey
- @KGGSEnglish--curriculum account, active
 - Run by Cat Garner
- Friends of KGGS Facebook page--school account, active
 - Managed by Zoe Anderson
- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be authorised by the IT Manager.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- Students running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation. Any student-run social media account will be supervised directly by a member of staff, who will have full access at all times, and will countersign the policy.
- Official social media use will be in line with existing policies.
- Images or videos of students will only be shared on official social media sites/channels in accordance with the image use policy.
- Official social media sites will be suitably protected (e.g. password protected) and where possible, run and/or linked to from the school website and take place with prior authorisation.
- I.T. staff must be aware of account information and relevant details for social media channels in case of emergency and for accountability.
- 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.

3.3 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 school Acceptable Use Policy and KGGS 'Basic Expectations'.

All members of staff are advised;

- a) Not to communicate with or add as 'friends' any **current** students via any **personal** social media sites, applications or profiles.

- b) Any pre-existing relationships or exceptions that may compromise this will be discussed with the Designated Safeguarding Lead or the Head teacher.
 - c) If contact with former pupils is required once they have left the school roll and they are at least 21 years of age then members of staff will be expected to apply their own professional judgement when using their personal social media sites for communication. If an exception is required for personal or professional reasons before the age of 21, approval must be sought from the Headteacher in writing. Staff should remember that they are still a representative of this school and therefore should moderate the content of the site to ensure confidentiality at all times.
- All communication between staff and members of the school community will take place via the official approved communication channels.
 - Under no circumstances should any user engage in private communication with a student through any social media platform. Exception is made only for a user to reply once to a received message that they will not communicate on the platform and that all messages should be sent to a school email address. Should a student continue sending messages after this point, they are to be ignored and referred to the Designated Safeguarding Lead.
 - There may be an occasion when contact with external agencies is easier through private messaging (e.g. no email address readily available). In these instances, and only in the case of external and adult parties, a user may use private messages to obtain an email address through which communication may continue. The preference is strongly and always to move the conversation to school email as soon as possible, in order to comply with data protection and oversight.
 - 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, colleagues etc. will not be shared or discussed on personal social media sites, in accordance with the EU General Data Protection Regulation.
 - All members of staff are strongly advised to safeguard themselves and their privacy as far as is feasible when using social media sites. Staff should use their judgement in balancing their needs with the need for privacy.
 - 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 schools policies and the wider professional and legal framework.
 - Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
 - Members of staff will notify SLT immediately if they consider that any content shared by anyone conflicts with their expectations of professional behaviour.
 - Members of staff are encouraged not to identify themselves as employees of KGGS 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 and the wider community.
 - Members of staff will ensure that they do not represent their personal views as that of the school on social media.
 - School email addresses will not be used for setting up personal social media accounts.

- Members of staff who follow/like the school's social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries and to protect their privacy.
- Staff should not make any comments about any members of the school community or their actions online, publicly or privately, whether named or implied. Failure to adhere to this instruction will be considered to be an act which breaches the AUP as well as the Teachers' Standards regulations.

3.4 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- Staff using social media officially will disclose their official position but always make it clear that they do not necessarily speak on behalf of the school.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel have appropriate parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the Head teacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with students or parents/carers through social media and will communicate via official communication channels.
- Staff using social media officially will sign the school's social media Acceptable Use Policy.

3.5 Pupils use of social media

- Safe and responsible use of social media sites will be outlined for students and their parents as part of the Acceptable Use Policy.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

- Pupils will be advised on appropriate security on social media sites and will be encouraged to use secure passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school where possible.
- 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 within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies.
- In order to protect their privacy, pupils should not interact with official social media accounts but only view them.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among students and adults will require all members the KGGS community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices is covered in the appropriate policy including the school Acceptable Use and Mobile Phone Policy.
- KGGS recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately.

4.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
- Electronic devices of all kinds that are brought into school or are taken on a school trip are the responsibility of the user at all times. KGGS accepts no responsibility for the loss, theft or damage of such items. Nor will KGGS accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- Mobile phones and personal devices are not permitted to be used within the KGGs site at any point during the official school day, unless prior permission has been given by a member of staff.
- Mobile phones and personal devices should not be used by any member of staff to record images in changing rooms or toilets unless SLT has given permission or there are no students present.
- Members of staff will be issued with a work phone number and email address where contact with pupils of parents/carers is required. Staff should not provide personal contact details under any circumstances unless SLT has given permission.
- All members of the KGGs community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the KGGs community will be advised to use lock screen mechanisms (e.g. PIN, pattern, TouchID) to protect their privacy and ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the KGGs community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school's policies.
- Mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of KGGs staff.

4.3 Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by students will take place in accordance with the acceptable use policy.
- Pupil's personal mobile phones and personal devices should be kept in a secure place, switched off and kept out of sight during the official school day. The only exception is for SEND students where the use of a phone is explicit in the Student Support Plan,
- Personal devices (including laptops, tablets, phones etc.) will only access the internet over the filtered & logged guest wireless provision during the school day, and must not use Virtual Private Networks (VPNs) or other mechanisms to circumvent filtering. This provision is available to KS5 students; KS3&4 students are therefore not to access the internet on personal devices during the day.
- If members of staff have an educational reason to allow students to use their mobile phones or personal devices as part of an educational activity, then it will only take place when approved by SLT.
- If a student needs to contact her parents/carers they will be allowed to use a school phone, a personal mobile phone may be used with explicit staff permission.
- Parents should not contact their child via their mobile phone during the school day, but should contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the headteacher.

- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the schools behaviour, safeguarding or bullying policy or could contain youth produced sexual imagery (sexting).
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

4.4 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting students, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with SLT.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with students and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.
- Staff personal mobile phones and devices will be switched to 'silent' mode during lesson times and staff will not answer their phones except with prior SLT permission.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of SLT.
- Staff will ensure that any content brought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy, then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the KGSs allegations management policy.

4.5 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school/settings acceptable use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- Emerging technologies will be examined for educational benefit and SLT will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. Currently this includes (but is not necessarily limited to):
 - Smoothwall Web Filtering
 - checks hourly for blocklist updates
 - is fully configurable by IT staff
 - Keeps web activity logs for 6 months
 - Generates a daily safeguarding report of suspicious activity
 - Outlook and Barracuda malware filtering and spam filtering to examine incoming email
 - IT staff can gain full access to any user's mailbox
 - LanSchool, classroom monitoring software
 - Allows staff to monitor student activity in a computer lesson
 - Also allows fine-grained controls for internet access if required
 - Monitors for keywords that might be cause for concern (e.g. suicide, bullying) and captures appropriate evidence, either a screenshot or a short recording; this captured evidence is accessible by IT Staff and will be shared with Pastoral and/or SLT where relevant
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.

- The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the school’s SLT.

5.2 Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school’s devices and systems for a period of six months.
- All staff and pupils will read and sign the Acceptable Use Policy as soon as is reasonably possible before using any school resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access (summary version) and discuss it with their daughter where appropriate.

6. Engagement Approaches

6.1 Engagement and education of students

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety (e-Safety) will be included school curriculum, covering both safe school and home use.
- Acceptable Use expectations and posters will be posted in all IT rooms.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.

6.2 Engagement and education of students considered to be vulnerable

- KGGS is aware that some students may be considered to be more vulnerable online due to a range of factors.

- KGGs will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked after Child Coordinator).

6.3 Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could 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.
- Members of staff with a responsibility for managing filtering systems or monitoring ICT use will be supervised by SLT and will have clear procedures for reporting issues or concerns.
- The school will highlight useful online tools which staff should use according to the age and ability of the pupils.

6.4 Engagement and education of parents and carers

- KGGs recognise that parents/carers have an essential role to play in enabling students to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their daughters.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their daughters online

7. Managing Information Systems

7.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the EU General Data Protection Regulations.
- Full information regarding the schools approach to data protection and information governance can be found in the school's Data Protection Policy.

7.2 Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may only be used for personal data when encrypted; the system will enforce this requirement automatically for staff.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices and personal devices through the school connection via the Smoothwall web filter, which stores logs for 6 months.
- Hacking is a risk for all social media profiles, where hacking may include:
 - A password being guessed
 - A password being stolen through social engineering (phishing)
 - A password being intercepted by malware (keylogging)
 - A password being stolen by a security failure on the platform (e.g. a database dump)
 - Access to the account having been gained via one of the above mechanisms (or any other), the password potentially then being changed to prevent the authorised user regaining control of the account
 - Unauthorised content potentially then being posted on the account
- If a user responsible for an official social media channel becomes aware that an account has been hacked, they should immediately change the password on said account. We strongly recommend users use a unique

password for any official social media channel but if this password is re-used elsewhere, it should also be immediately changed there. The password used on the email account linked to the social media account should never be the same.

- If access to the account has been blocked via an unauthorised password change, a reset password email should be used to regain access. This is why the email and social media accounts should not share a password, and why only school email addresses should be used to sign up for a platform, as this allows the school greater control in regaining access.
- If any unauthorised postings were made by the attacker, these should be deleted and an apology posted.
- Hacking is potentially also a risk for the school website; in this instance, IT Support will escalate to the website provider for their assistance in regaining control and restoring from backup, as well as analysing the website for potential malware/virus delivery and identifying the security flaw that allowed the unauthorised access.

Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- All pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system, a minimum of 12 characters long.

7.3 Filtering and Monitoring

- The governors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit student's exposure to online risks.
- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- All monitoring of school owned systems will take place to safeguard members of the community.
- 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.
- The school uses a Smoothwall web filtering system which blocks sites and content that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc. A list of the content categories filtered may be requested from the IT Support team; it changes too frequently to be listed here.

- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of via the AUP.
- If staff or pupils discover unsuitable sites, the URL will be reported to the IT Support team and will then be recorded and escalated as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from SLT.
- All changes to the school filtering policy will be logged and recorded.
- SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Lincolnshire Police or CEOP immediately.

8. Responding to Online Incidents and Safeguarding Concerns

- KGGS is conscious that the student body is vulnerable to image based sexual harassment (IBSH) and image based sexual abuse (IBSA). KGGS encourages a culture of disclosure and trust to allow concerns to be reported to staff (either directly or indirectly through peers), and that any such concerns will be listened to with respect and subtlety.
- All members of the community will be made aware of the range of online risks that are likely to be encountered including IBSH, IBSA, online-/cyber-bullying etc. This will be highlighted within staff training and educational approaches for pupils.
 - image-based sexual harassment (IBSH) describes two forms of digital sexual violence: (a) unwanted sexual images (e.g. cyberflashing, unsolicited sexual imagery); (b) unwanted solicitation for sexual images. "Images" are defined broadly to encompass all visual content, including photographs, videos, live chat etc.
 - image-based sexual abuse (IBSA) refers to the non-consensual recording, distribution, and/or threat of distribution of nude or sexual images. Although sometimes referred to as "revenge porn", IBSA encompasses many other contexts in which abuse can take place.
- KGGS is aware that IBSH overwhelmingly impacts girls and will plan and act accordingly to create a trusting and positive relationship between students and staff to encourage safe and honest disclosure. The school will also work to provide the social, emotional and mental health support for students experiencing IBSH.
- All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, IBSH, IBSA, cyberbullying, illegal content etc. Students will be encouraged to report concerns via any person or means they find most comfortable. Full details of the reporting procedure can be found in the Safeguarding Policy.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Lincolnshire Safeguarding Children Partnership(LSCP) thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.

- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the Head teacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Lincolnshire Safeguarding Team or Lincolnshire Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Lincolnshire Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Lincolnshire.
- Parents and carers will need to work in partnership with the school to resolve issues. The school will work to make parents and carers aware of the particular challenges and risks their children face online in order to encourage a trusting and positive dialogue between all members of the community.

Appendix A

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- KGGS will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- KGGS views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

- The school will follow the guidance as set out in the non-statutory UKCCIS (UK Council for Child Internet Safety) advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and LSCB (Lincolnshire Safeguarding Children Board) "Responding to youth produced sexual imagery" guidance
- If the school are made aware of an incident involving creating youth produced sexual imagery the school will:
 - Act in accordance with the school's child protection and safeguarding policy and the relevant Lincolnshire Safeguarding Children Boards procedures.
 - Immediately notify the designated safeguarding lead.
 - Store the device securely.
 - Carry out a risk assessment in relation to the student(s) involved.
 - Consider the vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies)
 - Make a referral to children's social care and/or the police (as needed/appropriate).
 - Put the necessary safeguards in place for the student e.g. offer immediate protection, counselling support and appropriate pastoral support for those involved.
 - Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.
 - Review the handling of any incidents to ensure that the school is implementing best practice and SLT will review and update any management procedures where necessary.
 - Inform parents/carers about the incident and how it is being managed.
- The school will not view any images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead and the Head teacher).
- The school will not send, share or save content suspected to be an indecent image of a student and will not allow or request other students to do so.
- If an indecent image has been taken or shared on the school network or devices then the school will take action to block access to all users and isolate the image.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- KGS will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- KGS views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team or Lincolnshire Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the Education Safeguarding Team or Lincolnshire Police by the DSL.
- If the school is made aware of an incident involving online child sexual abuse then the school will:
 - Act in accordance with the school's child protection and safeguarding policy and the relevant Lincolnshire Safeguarding Children Board's procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store any devices involved securely.
 - Immediately inform Lincolnshire Police via 101 (using 999 if a child is at immediate risk)
 - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
 - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
 - Make a referral to children's social care (if needed/appropriate).
 - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
 - Inform parents/carers about the incident and how it is being managed.
 - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

- KGGS will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent accidental access to Indecent Images of Children (IIOC) for example using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Lincolnshire Police.
- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
 - Act in accordance with the schools child protection and safeguarding policy and the relevant Lincolnshire Safeguarding Children Boards procedures.
 - Immediately notify the school Designated Safeguard Lead.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Lincolnshire police via 101 (using 999 if a child is at immediate risk) and/or the LADO (Local Authority Designated Officer) if there is an allegation against a member of staff.
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then 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.
- If the school are made aware that indecent images of children have been found on the schools electronic devices then 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 social 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 only.**
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
 - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
 - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
 - Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately.

9.5. Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of KGGs community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Lincolnshire Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.

- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
 - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
 - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
 - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
 - Parent/carers of pupils involved in online bullying will be informed.
 - The Police will be contacted if a criminal offence is suspected.

9.6 Responding to concerns regarding online hate

- Online hate at KGGS will not be tolerated. Further details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online hate reported to the school will be recorded.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
- The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Lincolnshire Police.

Appendix E

Online Safety (e-Safety) Contacts and References

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.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

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/online-safety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: <http://www.mariecollinsfoundation.org.uk/>

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: <https://360safe.org.uk/>

Online Compass (Self review tool for other settings): <http://www.onlinecompass.org.uk/>

Configuration History

Version:	Date:	Author	Contributors
1.0	November 2017	Mr P Mayfield, Mr M Dovey	Mr D Scott, Mrs J Lennie, Mr N Layhe
2.0	January 2020	Mr P Mayfield, Mr M Dovey	Mrs T Doig
3.0	January 2022	Mr M Dovey Mr P Mayfield	Mrs T Doig

Audit trail of change

Version	Date	Reason for Change
1.0	November 2017	New Policy
2.0	January 2020	Scheduled review
3.0	January 2022	Policy review

Authorisation by Welfare Committee

Name	Date	Signature
Mrs A Dorkes	February 2022	