

ICT Acceptable Usage Policy

Policy Number: N110

Policy Owner: Network Manager

Governing Body Responsibility: Resources Committee

Version: 6.1

Date: June 2022

Policy to be reviewed on or before June 2024



Kesteven and Grantham Girls' School

Contents

This policy is comprised of the following sections, which together comprise a complete document and should not be separated. The only exception to this is that versions missing one of either Appendix 2 or Appendix 3 may be produced for distribution to a targeted subset of users within the school e.g. a version may be compiled with only Appendix 2 and not Appendix 3 for distribution to staff. For the purposes of readability, “Kesteven & Grantham Girls’ School Acceptable Use Policy” is shortened to “KGGS AUP” below and throughout the policy.

- KGGS AUP – Overriding Principles
- KGGS AUP – Use of School Equipment
- KGGS AUP – Use of the School Internet Connection
- KGGS AUP – Use of Personal Equipment in Relation to School Activities
- KGGS AUP – Data Protection

- Appendix 1 – Definition of Terms & Legal Basis
- Appendix 2 – Staff Amendments & Agreement
 - 2A – Staff Amendments*
 - 2B – Staff Summary & Agreement*
- Appendix 3 – Student Amendments & Agreement
 - 3A – Student Amendments*
 - 3B – Student Summary & Agreement*
- Appendix 4 – Current Licensing Agreements for Copyrighted Material

Other related documents that Users should familiarise themselves with are:

- KGGS Data Protection Policy
- KGGS Service Level Agreement
- KGGS Mobile Phone Policy

Table of Contents

Contents	2
KGGS AUP – Overriding Principles	6
1. Aims and Principles of this Policy.....	6
2. Application of the Policy	6
3. Responsibility for this Policy.....	6
4. Personal Responsibility	7
KGGS AUP – Use of School Equipment	8
5. Acceptable Use	8
6. Purpose of the Network	8
7. Security, Honesty & Privacy on the Network	8
8. Transmission of Private Files	9
9. Security of the Network	9
10. Unauthorised Software	10
11. Unauthorised Hardware	10
12. Rights of the ICT Support Team on the Network including Monitoring of Activity 10	10
13. The Use of School Equipment Off-site.....	11
14. The Use of Copyrighted Material	12
15. Material Allowed on the School Network	12
16. Format Shifting	12
KGGS AUP – Use of the School Internet Connection.....	13
17. Acceptable Use	13
18. Purpose of the School Internet Connection	13
19. Security, Honesty & Privacy on the School Internet Connection.....	13
20. Security of the Network with regards to the School Internet Connection 14	14
21. Dissemination of Personal Details	14
22. Filtering of the School Internet Connection	14
23. The Use of Messaging Services including Chat Rooms.....	15
24. Online Communication including Forums and Email.....	15
25. The Posting of School-Related Material Online	15
KGGS AUP - Use of Personal Equipment in Relation to School Activities.....	16
26. Permission to Use Personal Electronic Equipment.....	16
27. Use of Personal Equipment to Circumvent Security or Damage the Network 16	16

28.	Health & Safety Implications of Personal Equipment.....	16
29.	Data Protection Implications of Personal Equipment.....	16
30.	The Use of Personal Recording Equipment.....	17
31.	The Use of Mobile Phones as Recording Equipment	17
32.	The Use of Personal Data Storage Devices	17
33.	The Security of the Network including the Intentional or Accidental Transmission of Malicious Code.....	17
34.	Responsibility for Personal Devices	18
35.	Provision of Services for Personal Devices	18
Appendix 1 – Definition of Terms		20
36.	Definition of Terms	20
37.	Definition of Inappropriate Material.....	21
38.	Definition of Misuse.....	21
39.	Definition of Anomalous or Suspicious Activity	21
40.	Definition of Publicly Accessible	21
41.	Legal Basis of this Policy	22
Appendix 2 – Staff Amendments		25
42.	Responsibility for Adherence to this Policy	25
43.	Potential Repercussions for Contraventions of this Policy	25
44.	Exceptions to the Inappropriate Materials and Misuse Clauses	25
45.	Definition of Reasonable Personal Use	26
46.	Accessing Student files	26
47.	Dissemination of Personal Details	26
48.	Responsibility for Data Protection	27
49.	The Use of Messaging Services including Chat Rooms.....	27
50.	Online Communication including Forums.....	27
51.	Contact with Students Outside School	27
52.	Permission to Use Personal Equipment.....	28
53.	Monitoring of Staff Activity	28
Appendix 2B - ICT Acceptable Usage Policy.....		29
Appendix 3A – Student Amendments		32
54.	Responsibility for Adherence to this Policy	32
55.	Potential Repercussions for Contraventions of this Policy	32
56.	Exceptions to the Inappropriate Materials and Misuse Clauses	32
57.	Definition of Reasonable Personal Use	32
58.	Security, Honesty & Privacy on the Network.....	33

59.	Dissemination of Personal Details	33
60.	The Use of Messaging Services including Chat Rooms.....	33
61.	Permission to Use Personal Equipment.....	33
62.	Mass Communications	33
Appendix 3B - ICT Acceptable Usage Policy.....		34
Appendix 4 – Current Licensing Agreements for Copyrighted Material		37
63.	Public Video Screening License (PVSL).....	37
64.	Performing Rights Society (PRS) for Music License	37
65.	Phonographic Performance Limited (PPL) License	37
66.	Educational Recording Agency (ERA) License.....	38
67.	Copyright Licensing Agency (CLA) License	38
68.	Motion Picture Licensing Company (MPLC)	38
69.	Schools Printed Music License (SPML).....	39
70.	Christian Copyright Licensing International (CCLI)	39
Configuration History		40

KGGS AUP – Overriding Principles

1. Aims and Principles of this Policy

This policy is designed to protect the Students, the Staff and the School and to prevent damage (temporary or permanent) being done to the careers and reputations of said parties. It forms both a basis for disciplinary action in the event of severe transgressions but also guidelines for the successful and safe use of ICT within school and in the pursuit of School Activities. By following this Acceptable Use Policy you will be contributing towards the success of the school ICT systems and allowing it to operate to the best of its capacity.

2. Application of the Policy

The Policy will apply to Students and Staff alike with different exceptions made between each group with respect to their anticipated needs and activities and the protection required for each group. These exceptions will be listed in two (2) documents exclusive of each other, namely the Student Amendments and the Staff Amendments. Exceptions may also be made for certain members of Staff and will be listed as part of the Staff Amendments document.

Amendments to this policy or any related policies considered part of this overall policy may be made at any time with the approval of the Board of Governors. All Users will be informed of changes to the document at least one (1) week in advance of those changes coming into effect, except in the most exceptional of circumstances at the discretion of the Board of Governors. These changes will not require an agreement to be signed again unless the Policy is significantly revised, at the discretion of the Board of Governors.

Anyone not agreeing to this policy will not be permitted access to the computer systems within the School and must not attempt to use any other User's credentials to gain access. Any attempt to do so will be met with the appropriate Disciplinary Measures in accordance with the Disciplinary Procedures.

Use of the school computer systems implies acceptance of this policy and all related documents.

3. Responsibility for this Policy

This Policy shall be administered on a day-to-day basis by the ICT Support Team under the guidance of the Network Manager. Any transgressions will be referred to the Network Manager for investigation by the ICT Support Team.

Amendments and improvements to this Policy will be made in consultation with the Senior Management Team and with the ratification of the Board of Governors.

4. Personal Responsibility

All Users within the School are provided with a personal account (technically referred to as a Domain Account) solely for their use. You agree that you are responsible for all activities done using this account (including any equivalent cloud services account, such as an email account, connected to this domain account). You therefore take responsibility for the security of your own account including the secrecy of your password and the locking/logging out of computers/accounts when they are not in use for any amount of time. Any transgressions against this policy performed on an account will be deemed to be the actions of the owner of said account.

It is also your responsibility to report any anomalous or suspicious activity to the ICT Support team and to facilitate their investigation in any way they may request in order to resolve the matter in a timely and professional manner. Anyone unnecessarily blocking an investigation being made by the ICT Support team will be deemed to be in contravention of this policy and will be open to such Disciplinary Procedures as are deemed appropriate by their superiors.

“Anomalous or suspicious” activity is defined in Appendix 1 and is subject to revision on a regular basis as deemed necessary and ratified by the SLT and Board of Governors. This also includes misuses of School Equipment and/or the School Connection that would qualify as a transgression by the terms of this policy.

KGGS AUP – Use of School Equipment

5. Acceptable Use

Users agree not to misuse the Network in any manner as defined in Appendix 1, Section 38.

Users also agree to treat the Network with respect, and recognise that any attempts to damage the Network physically or logically contravene this policy and will result in Disciplinary Measures being taken.

6. Purpose of the Network

Users agree to use the Network in a manner pursuant to the education of the Student Body. Provision is made for reasonable personal use where this does not interfere with the education of the Student Body. Such interference will be defined separately for Staff and Students in the relevant Amendments documents (Appendices 2A and 3A respectively)

The use of school equipment for business activities that are not related to the School is strictly forbidden. Personal commercial use is still acceptable within the bounds of reasonable personal use.

7. Security, Honesty & Privacy on the Network

No User will attempt, by any means, to impersonate any other User or to gain unauthorised access to any material that another User would reasonably expect to be private within the Network, for example gaining access to another User's home directory or email. No attempt will be made to steal or guess any password or otherwise circumvent password security on any system in place on the Network.

Each User is responsible for the security of their account and under no circumstances will the first party allow another User use of the first party's account. This includes (but is not limited to) the sharing of passwords in any form, or allowing another User to use a computer once the first party has logged on. Allowance is made for 2 (two) or more Users necessarily sharing a computer under supervision where resources are limited or where the work necessitates it, but no User should leave another User alone at a computer that the first party is logged onto. Allowance is also made for informing a member of the ICT Support team of a password in order to assist ICT Support in resolving any issues the User is experiencing.

Unless authorised by the authoring User, no electronic content stored on the Network should be viewed by another User or used in part or whole for any means. Authorisation should be given in written form by the original author. Another User may state explicitly that this authorisation has taken place but is then responsible for their assertion and may be subject to Disciplinary Procedures if this assertion is disputed by the original author and found to be false. In the event of a dispute the onus will be on the User transmitting the document to prove they had prior permission from the author for their actions and statements. An example of this authorisation would be wording to the effect of "*X has asked me to pass on the attached document*". Authorisation is implicit when a document is placed in a publicly accessible file storage area that is known to be available to a group of people, such as shared Student or Staff areas. An explanation of "publicly accessible" is defined in Appendix 1 of this document.

Similarly any User saving or copying any work to a shared file storage area therefore implicitly authorises any other User with access to that shared file storage area the rights to open and view the file. Should such a file need to remain private (e.g. work saved in the Submissions folder) then the User should password protect the file and inform the intended recipient of the password.

Please note that by saving any material onto the Network you are also implicitly authorising the ICT Support team access to this material in the pursuance of such activities as may be deemed necessary to support or improve the Network, or in the case of an investigation. Such access will only be undertaken where there is a demonstrable need to access the files or where instructed to by Senior Management when sufficient cause is believed to exist.

No User will impersonate any other person or entity that might exist outside of the School, or attempt to falsely affiliate themselves with any external person or entity, or otherwise falsely misrepresent themselves in any fashion.

No User will modify, delete, duplicate or transmit any content without authorisation from the original author, including (but not limited to) content in publicly accessible file storage areas or any content on removable media owned by another User where that removable media is on the school premises. Permission is implicit for ICT Support to archive a User's files once a User has left and remove said files from the network file storage.

8. Transmission of Private Files

No User will distribute a file or content they did not author to an audience not intended by the original author. The intended audience may be inferred on the basis of how the file was originally distributed, as detailed more explicitly in Appendix 1, "Definition of Publicly Accessible". Any transmission of files or content to parties not implicitly authorised by the author will be considered a transgression of this policy.

The body of an email is considered content for the purposes of this policy. For example, emails forwarded on with previous correspondence left below would fall under this restriction, and thus any prior conversation should be removed below the relevant message(s) before being sent on, unless: permission from the original author of those email(s) has been given; or the previous correspondence forms an integral part of the current message.

ICT Support may provide copies of files or content to law enforcement or agencies related to law enforcement or child protection in the event of an investigation with the knowledge of senior leadership.

9. Security of the Network

No User will knowingly introduce malicious software or code (including viruses, Trojans, rootkits and any other code which can be demonstrated to have a negligent effect on the Network) into the Network by any means; nor will any User use any software which introduces a reasonable risk of said malicious software or code to the Network (for example, P2P software).

The Network will have protection measures in place in order to mitigate the risk of such malicious software or code which will operate automatically and without the intervention of the User. Therefore no User will interfere with or otherwise interact with such solutions in any way that would harm the security of the Network, including disabling the protection measures for any reason, or in any way attempt to circumvent any security measures in place on or in the Network. In addition no User will attempt to implement any other solutions on the Network as these may interfere with the correct running of the Network as configured, contravene licensing agreements for such software, or be malicious software or code misrepresenting itself as protection software. This includes standalone software that may attempt to install from a file or software or code that may run from malicious websites.

10. Unauthorised Software

No User shall install any software of any kind on any part of the Network. Any software that is required for School Activities must be passed to the ICT Support team for testing, approval and installation. Any software desirable to improve the performance or stability of the Network will be decided on solely by the ICT Support team and is not within the remit of any other User.

No User shall execute any software not already provided on the Network by ICT Support or otherwise approved by them in writing.

Unauthorised software is both a security risk and a legal risk as license agreements are restrictive in the use of software. "Free" software is often only free for personal use, which excludes use in a public setting such as a school. Breaking these License Agreements opens up the School to legal action where the School will be held responsible.

11. Unauthorised Hardware

No User shall install any hardware of any kind on any part of the Network. Any hardware purchases must be made with the awareness and advice of the ICT Support team and installed by the ICT Support team in order to facilitate the continued support of any hardware. Unauthorised hardware could pose a security risk to the Network.

Personal hardware is covered in sections 26 to 33, "[KGGS AUP – Use of Personal Equipment in Relation to School Activities](#)".

12. Rights of the ICT Support Team on the Network including Monitoring of Activity

By accepting this Policy you agree that all files saved on the system may be viewed or accessed at any time by the ICT Support team in pursuance of its responsibilities, including (but not necessarily limited to) the maintenance and improvement of the Network and the investigation of any breaches of this Policy.

No unnecessary access will be undertaken in accordance with the Service Level Agreement that the ICT Support team operates by.

ICT Support may review server logs to determine email activity at any time; these logs do not display the body of the email or any attachments, only the subject of any emails as well as sender and recipient information, relevant timestamps and other technical data. ICT Support may also access your email mailbox without your knowledge in pursuit of a disciplinary investigation with the written authorisation of Relevant Superior Parties as defined in Appendix 1.

By accepting this policy you also agree for all of your activity to be monitored for contraventions of this policy or UK law or international law where relevant. This monitoring will include a dedicated keyword system (currently Impero) that will store screenshots, potentially screen recordings, and technical details of activity when it automatically detects words it believes to be of concern. This system is reviewed regularly by members of ICT Support and Pastoral and issues flagged up by it may be raised with the Relevant Superior Parties, possibly including law enforcement. This system stores captures indefinitely, and data cannot be erased from the system. You agree that in the event of any detected criminal activity on the Network that the Police or other designated legal body in pursuit of their investigations may be provided materials as evidence and that any recorded activity (whether relevant to the investigation or not) will as a matter of consequence be in the possession of said third party.

Computer classrooms also have management software installed to allow staff to monitor and control the activity of Users in that room from the designated teacher's workstation in that room.

Any attempt to circumvent any monitoring or management software will be considered a precursor to activity that further contravenes this Policy and is a severe transgression of this Policy. The User will then be subject to the relevant Disciplinary Procedures.

13. The Use of School Equipment Off-site

Any User who, as part of their school work, takes any ICT equipment owned by the School off-site agrees to continue abiding by the contents of this Policy with regards to that equipment. The User agrees that said equipment will only be used in the pursuance of School Activities and will not use said equipment for purposes other than official school business.

Any User in possession of school equipment is solely responsible for that equipment at all times until formally returned to ICT Support. Any damage to or loss of equipment may be charged to that User at the discretion of senior leadership.

Equipment must also be returned in a timely manner at the request of ICT Support to undertake regular maintenance and checks. Senior leadership may also request that equipment be returned permanently to the School if they deem it no longer essential to the User, and said User will then formally return it to ICT Support in a timely manner.

Users are asked to take particular note of sections 10 ([Unauthorised Software](#)) and 11 ([Unauthorised Hardware](#)) with regards to school equipment entrusted unto them.

14. The Use of Copyrighted Material

In order to ensure the School's compliance with the Copyright Designs and Patents Act 1998 Users agree not to broadcast or use copyrighted films, music, television programming, images or text except where the School is specifically licensed for the intended material and purpose.

The only purpose for which such materials can be used under the Fair Use provision in law is where the material is educational and relevant. As an example, a piece of music can be used if it is the subject of study by a class, but it cannot be used simply as background music as this constitutes public broadcasting and is not protected under the Fair Use provision. Similarly a film can be shown if it is relevant to a book being studied in English, but cannot be shown simply as entertainment at the end of a term.

Licenses may be obtained and held by either the School or the Department for Education that provide legal exceptions to the rules above. These exceptions are detailed in Appendix 4.

15. Material Allowed on the School Network

Users will not save picture, music or video files to the Network in any location unless there is an explicit need for the pursuance of a School Activity. Space on the Network is limited and it is intended for Users to save work and pursue their education, not to serve as a media store for Users. This is particularly relevant with regards to section 14 ([The Use of Copyrighted Material](#)).

As such, any User found to be using the Network to store digital media that is not relevant to a School Activity that they are involved in will be deemed to be in contravention of this Policy and will be subject to Disciplinary Measures in addition to the files being deleted. Regular monitoring of this will take place.

16. Format Shifting

Users will seek the permission of the original author before creating a digital version of any material not already in that format on the school network. Examples include (but are not limited to) scanning in a letter provided only in physical format, scanning in a printed photo or creating an MP3 from a CD recording. Changes between different digital formats are permitted (e.g. bitmap to JPEG) but not where such a conversion would remove any protections or restrictions placed on the original file such as password protection or read-only protection.

KGGS AUP – Use of the School Internet Connection

17. Acceptable Use

Users agree not to misuse the School Internet Connection in any manner as defined in Appendix 1, Section 36.

18. Purpose of the School Internet Connection

Users agree to use the School Internet Connection in a manner pursuant to the education of the Student Body. Provision is made for reasonable personal use where this does not interfere with the education of the Student Body. Such interference will be defined separately for Staff and Students in the relevant Amendments documents (Appendices 2 and 3 respectively).

The use of the School Internet Connection for business activities that are not related to the School is strictly forbidden. Personal commercial use is still acceptable within the bounds of reasonable personal use.

19. Security, Honesty & Privacy on the School Internet Connection

No User will impersonate any other person or entity that might exist in- or outside of the School, or attempt to falsely affiliate themselves with any external person or entity, or otherwise falsely misrepresent themselves in any fashion.

No User will attempt, by any means, to gain unauthorised access to any material that they do not have the right to access, either by impersonation or other attempts. No attempt will be made to steal or guess any password or otherwise circumvent any security systems encountered on the Internet.

Unless acting in an authorised official position, all electronic communications undertaken through the School Internet Connection must be signed with the following text to prevent Kesteven & Grantham Girls' School being implicated in any complaint that may arise as the result of said electronic communications:

"This message is personal. The opinions expressed are in no way an official view of Kesteven and Grantham Girls' School (KGGS) neither should they be considered as an indication of KGGS policy unless explicitly stated otherwise."

This is required even for personal communications sent, through the school email provision or otherwise, as all communications sent through the School Internet Connection can be traced back to the School. Any emails sent from a school email account to an external address will have the aforementioned text automatically appended.

20. Security of the Network with regards to the School Internet Connection

No User will knowingly or otherwise visit any site that they suspect would represent a threat to the Network through the use of malicious code or software. Any User who wishes to access a site they are unsure of should contact the ICT Support team for assistance. Any User who inadvertently or otherwise connects to a site they suspect of representing a security issue must report the incident immediately to the ICT Support team for investigation and possible repair. The failure to report such an incident will be considered a transgression of this Policy; timely reporting of such an incident will mitigate any transgression against this specific part of the Policy such that no further action will be taken except in cases of demonstrable gross negligence.

The Network will be secured as far as is possible against such threats through the use of anti-virus software, firewall(s) and filtering software as a minimum. This will not eliminate the possibility of zero-day threats circumventing such measures; hence the User still has a responsibility to use the School Internet Connection in a safe and conscientious manner.

21. Dissemination of Personal Details

No User will disseminate any personally identifiable information about themselves including (but not limited to) full name, address, age, gender, occupation or other information considered to be personally identifiable.

22. Filtering of the School Internet Connection

The School Internet Connection is filtered automatically by software that checks against a blacklist of sites & keywords and makes automatic decisions based on the presence of key phrases or activity detected on the requested website. This filtering is required to ensure the safety of the Student Body and the security of the Network.

Any attempts to circumvent this filtering through the use of software, third-party proxies or any other means will be considered a precursor to further activity contravening this Policy and is a severe transgression of this Policy. This will result in Disciplinary Measures being taken against the User.

Due to the technical limitations of filtering solutions the system should not be considered 100% reliable. Any attempts to access material that the User suspects would otherwise be filtered (where the assumption can be derived from the contents of this Policy) will be considered a transgression of this Policy unless the User immediately reports the URL to the ICT Support team for the filter to be updated.

Similarly the filter may be overzealous in its blocking of sites as it is configured to err on the side of caution. If a demonstrable need for the website can be shown (with regards to a valid school activity) then requests can be made to the ICT Support team for the website to be unblocked. Should this request be found to be made for purposes other than the pursuance of School Activities then the User will be subject to Disciplinary Measures.

Users agree that as part of the filtering system implemented by the School that data will be collected on the browsing history of Users and may be analysed to improve the filter. This data will be personally identifiable and may be used to form part of an investigation into a User should it be deemed necessary to undertake such an investigation by Senior Management. This data will only be used internally and will not be shared with any external parties except as part of an investigation resulting in third parties necessarily becoming involved.

23. The Use of Messaging Services including Chat Rooms

The User agrees not to use any software, website or other system that allows for real-time messaging to be undertaken. This includes social networks (such as Facebook Messenger, Twitter Direct Messages etc.), purpose applications (e.g. Skype, Slack) and chat rooms available on websites (public or private). For the purposes of this Policy real-time messaging is defined to be the instant relay of messages to another party, typed, spoken or otherwise.

24. Online Communication including Forums and Email

The User agrees not to participate in any conversation through the School Internet Connection except when in relation to a School Activity, including the use of bulletin boards, message boards, forums, profile pages or any social networking site.

Users will not use a personal email account through the School Internet Connection whether accessed through a webmail portal or other means. A school email account is provided and this is the only email that should be used in School.

Users may have their email provision revoked or limited on a temporary or permanent basis at the written request of the Relevant Superior Parties.

25. The Posting of School-Related Material Online

The User agrees not to post any material online related to the School including any personal data or opinions on the School except where relevant to the pursuance of School Activities and sanctioned by Senior Management. No images or personal data shall be posted online without the express permission of Senior Management, who will ensure that all relevant guidelines regarding Data Protection are followed. This guideline includes the creation and/or updating of blogs, video blogs, forums or any other website allowing material to be posted publicly or privately including messages left on social networking sites.

For the purposes of clarity: it is forbidden to post any images, audio recordings or videos of students or staff online--anywhere--without the express permission of Senior Management. This applies regardless of where the image/audio/video was taken, that is, including images/audio/videos of school trips as well as material created on school premises.

Please note that this also applies to the User in their personal time when using equipment other than the school Network in order to protect the School.

KGGS AUP - Use of Personal Equipment in Relation to School Activities

26. Permission to Use Personal Electronic Equipment

Staff and Key Stage 5 students may bring personal laptops & tablets for their own study/work only. Such devices may only be connected to the *KGGS Guest* wireless network provided in school, which is segregated from the main school network and filtered appropriately.

Users should familiarise themselves with other policies or school rules that may be relevant to items of personal equipment, particularly policy N117 *Mobile Phone & other Electronic Devices Policy*

27. Use of Personal Equipment to Circumvent Security or Damage the Network

No User will use any personal electronic equipment in an attempt to defeat or circumvent the security of the Network, including the use of VPNs or personal Internet connections (e.g. 4G) to circumvent any filtering solution that the School has implemented. This includes (but is not limited to) the use of mobile phones to access the Internet outside of the filtered School Internet Connection, either directly or in hotspot mode.

No User will use any equipment to damage the Network physically or logically or in any way attempt to cause harm or present risk to the Network.

28. Health & Safety Implications of Personal Equipment

Due to Health & Safety legislation on Portable Appliance Testing (PAT Testing) any User bringing personal electronic equipment onto School property shall not allow any other User to make use of said equipment. By bringing personal equipment on site you are accepting the assumed risk of using said electrical equipment on site and absolving the School of any responsibility in the event of an electrical fault occurring in your equipment, including incidents that lead to personal injury or death.

29. Data Protection Implications of Personal Equipment

No User will keep the personal data of any other User on personal equipment without the express permission of the ICT Support Team and Senior Management, including digital images that allow other Users to be recognised and identified.

The taking of such personal data off site requires a separate permission to be granted by the ICT Support Team and Senior Management.

Any such personal data kept on digital storage will, where possible, be encrypted by the strongest means available to mitigate the potential loss of said data.

Users will take care not to mingle such personal data with their own private data in such a way that there is not clear delineation between the two sets of data. In the case of a file storage system, any such personal data must be kept in a separate folder that is clearly labelled to prevent confusion, and this folder then encrypted as noted above.

30. The Use of Personal Recording Equipment

It is recognised that Users will have occasion when they will want or need to use personal recording equipment (including but not limited to smartphones, cameras, camcorders and audio recording devices, analogue or digital) in the pursuit of School Activities.

In such an event the User will notify the relevant staff member (e.g. class teacher) or ICT Support Team in advance. Efforts must then be made to clearly separate such recordings as made in the pursuit of School Activities from any private recordings. It is recommended that where possible separate media (possibly provided by the school) is used for the storage of such recordings made in the pursuit of School Activities. For example, a teacher wishing to use a personal digital camera to record a school trip should use a memory card provided by the school for the duration of the trip and should provide adequate notice of their requirements.

The User must then return the personal equipment to the ICT Support Team immediately upon completion of the task or upon the Users return from such activities as have occurred off-site. The ICT Support Team will then download such media as has been recorded and provide it back to the User in whichever form is most relevant to the tasks the User wishes to accomplish.

31. The Use of Mobile Phones as Recording Equipment

Many mobile phones now feature the ability to make recordings of an audio and visual nature. Due to the added risk derived from the inherent nature of these devices, i.e. the ability to transmit and communicate such recordings, no mobile phone (or functionally equivalent device) shall be used to make any recordings of any other User or store any other User's personal data. Such devices may still be used in situations that do not involve any such personal data or recordings, e.g. for recording a User's personal art work in school.

This section may be overridden with explicit staff permission, in order that a student may record evidence of, or media for, school work.

32. The Use of Personal Data Storage Devices

The School allows for the use of personal data storage devices (including, but not limited to, USB pen sticks and external hard drives) in order to effectively relay files between a User's personal equipment off-site and the Network. Such devices may only be used to assist in the transfer of files relevant to School Activities, and must not feature any private data that is in contravention of any other part of this Policy (including, not limited to, copyrighted material that the School does not own and is not licensed to use and any inappropriate material as previously defined in this document). Personal data (as defined in the Data Protection Policy) must not be stored on unencrypted storage devices to avoid the risk of data breaches.

33. The Security of the Network including the Intentional or Accidental Transmission of Malicious Code

The User guarantees that any equipment brought on site and connected to the Network is free of viruses and other malicious code, including laptops or similar equipment or personal data storage devices that will be connected to the Network.

The ICT Support Team reserves the right to subject any such equipment to scans in order to protect the Network and identify and threats to the Network. As a result of such scans the ICT Support Team may install (with the User's knowledge) protective software on the User's personal equipment to ensure the continued suitability of the personal equipment for use in School. Such software as is installed will be free for personal use and incur no extra responsibilities or costs on the User or the School.

34. Responsibility for Personal Devices

Any and all personal devices brought onto school premises by a User remain the sole responsibility of that User and the School in no way accepts any liability for any loss or damage of any personal devices brought on site by a User. A User accepts all risks and responsibilities for bringing their personal devices into School. A User is responsible for all technical support of their personal devices and ICT Support is under no obligation to provide support to Users for said personal devices.

35. Provision of Services for Personal Devices

The provision of services for personal devices, including (but not limited to) wireless access to the Network and internet, are entirely at the School's discretion and may be revoked in part or whole at any time without prior warning. So long as sufficient access to resources deemed necessary by senior leadership and the governing body is made available to Users through the School Network, the School shall be in no way bound to provide any services for personal devices providing similar access to such services.

ICT Acceptable Usage Policy

Appendix 1

Definition of Terms



Kesteven and Grantham Girls' School

Appendix 1 – Definition of Terms

The lists defined in sections 36 through 40 are not exhaustive and it is expected that amendments will be made. Any activity deemed unsavoury that falls outside of the current definitions will be taken to Senior Management or the Board of Governors for a decision on whether said activity contravenes the spirit of this Policy.

36. Definition of Terms

The following terms may be used throughout this document and other related documents and are defined here for purposes of clarity.

“The Policy” refers to the Kesteven & Grantham Girls’ School Acceptable Use Policy as a whole, including all related documents that are noted in such documents as being a part of or operating alongside the Kesteven & Grantham Girls’ School Acceptable Use Policy.

“The Network” includes all hardware and software that together comprises the ICT provision inside Kesteven & Grantham Girls’ School, and any data stored on said hardware. **“School equipment”** refers to any hardware that constitutes a part of the Network.

The **“School Internet Connection”** refers to the method through which the School connects to the Internet, however that is currently implemented. It includes all filtering and proxy systems involved in this connection.

“Staff” includes all paid employees of the school, teaching and support, any unpaid volunteers working in the school under agreement, and any visitors to the School operating in an official manner who will have cause to come into contact with the Network in the performance of their on-site duties.

“Students” includes all girls on roll at Kesteven & Grantham Girls’ School and any other visiting students who are here in an educational capacity (including, but not limited to, visiting students from The King’s School).

“The Student Body” collectively refers to all Students who use the Network at any point, and is not necessarily limited to those Students who are currently on site at Kesteven & Grantham Girls’ School.

“The School” refers to Kesteven & Grantham Girls’ School, comprising of the site & facilities located on Sandon Road, the Staff and the Student Body, and the image and reputation of the School in the community.

“User” and the collective **“Users”** therefore refers to Staff and Students using the Network inside the School. Anyone who falls outside of the given definitions for Staff or Student shall not be permitted access to the Network in order to ensure the security and integrity of the Network.

“School Activity” includes all pursuits officially endorsed by the school, curricular and extra-curricular.

“Disciplinary Procedures” refers to the Kesteven & Grantham Girls’ School Disciplinary Procedures already in place for both the Staff and Students.

“Disciplinary Measures” therefore refers to actions taken as a result of following said Disciplinary Procedures.

“Third Party” refers to any external body including but not limited to law enforcement, parties working with or for the Local Education Authority or any external company contracted by the school to provide a service.

“Relevant superior parties” is defined for students as: a relevant subject teacher, form tutor, head of year, head of key stage, senior leadership and the Headteacher. ***“Relevant superior parties”*** is defined for staff as: head of subject, head of faculty, senior leadership and the Headteacher.

“Senior leadership” also explicitly includes the Headteacher as well as those staff designated senior leadership for the purposes of this policy.

37. Definition of Inappropriate Material

For the purposes of this policy, ***Inappropriate Material*** is defined as including (but not limited to) pornography, illegal material including unauthorised copyrighted material, racist, sexist or otherwise prejudiced and demeaning material, material or activity related to gambling (simulated or real), alcohol, drugs, terrorism, violence, material that may be harmful to the School Network such as viruses, or any other material which after consideration could be deemed to be unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone’s privacy, hateful or otherwise objectionable.

Please note that this definition is limited to the scope of this document and implies no expectations or definitions about material outside the scope of this policy, and that what may be deemed acceptable by this policy may be unacceptable in other areas of school policy.

38. Definition of Misuse

Misuse of the school network includes (but is not limited to) attempts to circumvent the security of the Network, including attempts to cause wilful damage to the Network, and the viewing, storing or transmitting of inappropriate material as defined in Appendix 1, Section 37.

39. Definition of Anomalous or Suspicious Activity

Anomalous or suspicious activity includes (but is not limited to) any unusual behaviour by the equipment or by another User that is outside the normal bounds of expected use and which you have reason to believe is (or will result in) a transgression of this policy. If you are in any doubt regarding such observations please seek advice from the ICT Support team for clarification and assistance.

40. Definition of Publicly Accessible

A publicly accessible file storage area is a shared folder made available to more than one person on the system and known to be available in such a manner. Such an area may be made available via a mapped drive or a shortcut provided to certain staff.

For these publicly accessible file storage areas, “public” is defined as the users who have access to this area. For example, a file saved to an area accessible to all staff but not to students should be considered public amongst staff but private with regards to students. Implicit authorisation from the author can only be inferred for the users who would normally have access to the file and any attempt to distribute such a file wider than this audience would be considered a breach of this policy and potentially of the Data Protection Policy.

Email inboxes are considered a privately accessible area, not publicly accessible. Where an email is sent to more than one person, the content of that email may be considered public amongst the recipients of that email. For example, an email sent to all staff may be considered public amongst the school staff, but private to students or external parties. This authorisation may only be inferred for attachments where the sender of the email is the author of the attachment. If an attachment is sent by someone other than the original author of that attachment then explicit mention of the permission to distribute that specific attachment must be made in the body of the email. If it is not, clarification should be sought in writing (e.g. an email reply) from the sender.

41. Legal Basis of this Policy

A number of laws govern the use of computer systems or cover activities relevant to the Network and Users. This Policy, when followed, ensures the School's compliance with these laws and protects us from legal action. Any breaches of this Policy may represent a breach of UK or International Law and may open up both the User and the School to criminal prosecution or civil action, incurring significant fines and/or jail time as a result.

The Acts considered particularly relevant with regards to this Policy are as follows:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1998
- Criminal Justice Act 1988
- Defamation Acts 1952 and 1996
- Freedom of Information Act 2000
- Human Rights Act 1998
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1988
- Protection from Harassment Act 1997
- Public Order Act 1986
- Race Relations Amendment Act 2000
- Telecommunications Act 1984 & 2000
- Data Protection Acts 1984 and 1998
- Sex Discrimination Act 1986
- Regulation of Investigatory Powers Act (RIPA) 2000

In particular, please note the following relevant points:

The Data Protection Act 2018 and the Regulation (EU) 2016/679 (General Data Protection Regulation) are the basis of the section “KGGs AUP – Data Protection”.

Computer Misuse Act 1990 states that it is illegal to intentionally gain unauthorised access to a computer or to data held on a computer, for any means, and it is illegal to make any unauthorised modification of a computer or data held on a computer.

The Telecommunications Act 1984 & 2000: Section 43 makes it an offence to send “by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character”. Please note that “public telecommunications system” includes both the Internet and the School’s Network.

Copyright, Designs and Patents Act 1988 provides a legal basis for the protection of intellectual property. This has connotations for the Network with regards to the use of unauthorised software or the illegal copying of software owned or licensed by the School for personal use. It also has repercussions for the use of material found on the Internet, as unless explicitly noted by the author on the source page all material is automatically copyrighted under European law and cannot be used without permission.

ICT Acceptable Usage Policy

Appendix 2

Staff Amendments & Agreement



Kesteven and Grantham Girls' School

Appendix 2 – Staff Amendments

The following points are an addendum to sections 3, 4 & 5 of the KGGS AUP that are relevant to Staff only, including support Staff and any visitor on site who is performing duties on behalf of the school (such as supply Staff or external exam invigilators).

Appendix 2B should be read, understood & signed by each member of Staff and returned to the School for safe keeping.

42. Responsibility for Adherence to this Policy

Staff members are held accountable by their line manager, for example the Head of Faculty. If this line manager feels that a User is not adhering to this Policy they may instigate an investigation into the User with the approval of Senior Management and the assistance of ICT Support.

Similarly it is the responsibility of line managers to ensure that all Staff they are responsible for are adhering to this Policy, and any severe transgressions of this Policy by a User where the line manager was unaware may invoke repercussions for said line manager.

43. Potential Repercussions for Contraventions of this Policy

This Policy forms the basis for potential disciplinary action and sanctions can range from verbal warnings to dismissal. All disciplinary measures will follow the policies already in place in the School as agreed by all relevant Unions.

A formal warning system will be followed in the event of transgressions and will generally follow the pattern of:

- Verbal warning from line manager
- Written warning from line manager
- Written warning from the Headteacher
- Formal meeting with Headteacher & line manager
- Suspension
- Dismissal

For certain extreme incidents, particularly those relevant to Child Protection, some of the initial steps may be skipped in order to immediately reduce the risk to Students. Such action will only be undertaken with the consent of the Senior Management team and will be reviewed by the Board of Governors.

44. Exceptions to the Inappropriate Materials and Misuse Clauses

It is recognised that Staff will have occasion to visit websites containing material previously defined as Inappropriate Material in Appendix 1, Section 37. Such occasions may include (amongst others) the planning and execution of lessons covering subjects that touch on the listed materials (such as drugs-related websites). In such cases the Staff member in question should inform their Head of Faculty of such access being undertaken.

Should a Staff member require access to such a site for a School Activity and they find it is blocked by the school internet filter, they should make a request in writing (i.e. e-mail) to the ICT Support Team detailing the website, the reason and the period of time for which the rule is to be in place. The User's Head of Faculty should be copied in on this communication. It is recommended that teachers do this on behalf of their Students where it is anticipated that Students will need the website for independent research.

45. Definition of Reasonable Personal Use

In sections 6 and 18 of the main Policy, allowance is made for Users to access the school Network and use the School Internet Connection for personal use, within reasonable levels where this does not interfere with the education of the Student Body.

Such interference is defined as overuse to the point of other staff duties being neglected; for example, a teacher regularly late to lessons because of personal computer use, or missing school duties, would be deemed to be neglectful.

It is therefore expected that Staff will not use the Network for personal means inside a lesson that they are responsible for. Non-teaching periods may be used to take advantage of the school Network for personal means, but not at the expense of other duties such as marking that may be neglected as a result. Such guidelines will be used by the User's Head of Faculty and the SLT in the event of a Staff member becoming obviously neglectful.

Personal use must still be within the constraints of the other sections of this Policy.

"Personal commercial use" as allowed in sections 6 (Purpose of the Network) and 18 (Purpose of the School Internet Connection) includes the use of online shopping, booking & banking systems, and similar such systems. Should any commercial site accessed in the course of reasonable personal use later be deemed to be unsuitable by SLT and/or the Board of Governors, any use until that point will not be considered a breach of this Policy. Any commercial sites used must not contain any inappropriate material as defined in Appendix 1, Section 37

46. Accessing Student files

In addition to section 9 of the main Policy, which states that "Unless authorised by the authoring User, no electronic content stored on the Network should be viewed by another User or used in part or whole for any means", Staff members are authorised to view and use Student work in pursuance of their school duties. This includes accessing such files for marking or using Student work (in whole or part) to create displays or advertise exemplary work.

47. Dissemination of Personal Details

It is recognised that Staff will need to disseminate certain personal details in the pursuit of their school duties, such as submitting contact information to various companies. As such, whilst caution is still advised, this restriction is relaxed for members of Staff.

There are occasions when certain student details should not be disseminated, and the Assistant Headteacher with responsibility for child protection will provide a list of such students each year.

48. Responsibility for Data Protection

Contemporary data protection law places a greater responsibility than ever on the school. All staff share in this responsibility and are expected to consider data protection in all actions, particularly as regards students' personal data.

In particular, staff are not permitted to store files containing any student data (e.g. reports) on removable media (e.g. memory sticks) due to the risk of data loss. Write access to removable media will be blocked on the network from September 2018. Alternative technical provisions are available to access files over the internet and these should be used instead.

If staff use said provisions (e.g. Files, OneDrive) and download a copy of a file with student data in order to view or modify it, the device used should be password protected (or equivalent alternative for mobile devices e.g. fingerprint, pattern).

Student data should not be transmitted over non-work communication channels (e.g. WhatsApp). This is both for the protection of the data and to allow the school to comply with Data Subject Requests requiring the collation of data.

49. The Use of Messaging Services including Chat Rooms

Exceptions are made for Staff where such facilities are used by external support companies to offer support and/or sales advice.

Exception is made for such services as are automatically connected to a school account e.g. Microsoft Teams.

50. Online Communication including Forums

With reference to section 24 of the main Policy, staff are only restricted by this section during school hours. Exceptions are also made for Staff where such sites offer assistance in relation to School Activities or the preparation of School Activities.

The restriction on the use of personal email is also relaxed for Staff, although it is expected that such accounts are not used for school purposes. Personal email use is only allowed for non-school business where this falls within the guidelines defined in section 45 of this Appendix ([Definition of Personal Reasonable Use](#)).

Staff are not permitted to make statements about Students online in any form at any point, including in their own time. Even sending a private e-mail or message can constitute a case for libel as these messages are enough to satisfy the legal definition of "publishing".

51. Contact with Students Outside School

Teachers are not permitted to have direct contact with Students outside of School by any means except through their school e-mail address. This is to prevent any accusations of improper behaviour and protect both Staff and Students.

52. Permission to Use Personal Equipment

Staff may bring personal equipment on site for use with the Guest wireless network, which allows access to the internet only and not any internal services (including printing). As per section 34 of the main policy, staff are wholly responsible for their own equipment, and the school is not liable for any damage or harm that may arise from use on the network (e.g. a virus infection spread through the Guest network, which by its nature is outside the control of the IT Support department).

The restriction on personal audio players is relaxed for Staff. These devices may be used in lessons when they are plugged into speakers for the benefit of the class (following the restrictions in section 13 of the main Policy, The Use of Copyrighted Material), or used as personal devices in the User's free time.

Staff are reminded that any mains operated personal equipment must be fully PAT tested.

53. Monitoring of Staff Activity

Staff screen captures taken by the safeguarding system detailed in section 12 of the main policy will only be accessible by IT Support staff, and will only be accessed at the request of SLT where specific cause exists to review possible captures. (this page left intentionally blank)

Appendix 2B - ICT Acceptable Usage Policy**Summary of Acceptable Use Policy - Staff**

This document is intended as a readable summary of the KGGS AUP. You should still familiarise yourself with the full document as you are agreeing to abide by the full policy.

All Staff agree:

- To keep their account secure by not sharing their password or logon and by not leaving any computer they are logged onto unattended and open.
- To only use the network in a manner pursuant to the education of the student body, excepting reasonable personal use in their non-teaching time.
- To abide by all relevant UK laws when using the network
- Not to undertake any business activities, on or offline, except for the school.
- Not to use, view, store or transmit any inappropriate material as defined in the full policy except where necessary for lessons or other school activities.
- Not to allow any security risks to either the network or themselves, either from malicious websites (e.g. phishing scams) or malicious software (e.g. viruses).
- Not to (attempt to) circumvent any security, filtering or monitoring systems on the Network in any way.
- Not to use or install any software or hardware that has not been approved by ICT Support.
- To only use copyrighted material within the bounds of the school/county licensing.
- Not to post any comment or material online that is related to the school or any members of the staff or student bodies unless explicitly authorised by the Headteacher – including any private messages sent in personal time.
- Not to use any online chat facility (including Instant Messengers or chat rooms hosted on web sites) or use other online communications (such as forums) during school hours except where it assists with lessons or their preparation.
- Not to have any direct contact with students outside school except through school provided accounts such as email or Teams
- That any personal equipment brought on site may only be used by the owner and cannot be shared; it must also not endanger the network in any way. Staff are reminded that any mains operated personal equipment must be fully PAT tested.
- Any school data stored on personal equipment must be encrypted where possible and must not intermingle with private data.
- To abide by the Data Protection Act 2018 for all data collected on any member of the school for any purpose, including school projects and research.
- To consent to the processing & transfer of their data where relevant in accordance with the requirements of the School, the Department of Education and the LEA.

All Staff are aware that:

- Activity on the network and on the Internet is monitored for the safety of all users.
- All files and emails are accessible by ICT Support in the event of a request by SLT or the User in pursuit of supporting the network or investigating a security or disciplinary matter.
- Any breach of this agreement may lead to disciplinary action being taken

I have read and understood this policy:



Signed: _____ Date: _____

Printed Name: _____ Position: _____

Confidential Once Signed

Kesteven & Grantham Girls' School

(this page left intentionally blank)

ICT Acceptable Usage Policy

Appendix 3

Student Amendments & Agreement



Kesteven and Grantham Girls' School

Appendix 3A – Student Amendments

The following points are an addendum to sections 3, 4 & 5 of the KGGS AUP that are relevant to Students only, including visiting Students who have reason to access the Network (such as Kings' students).

Appendix 3B should be read, understood & signed by each student and returned to the School for safe keeping.

54. Responsibility for Adherence to this Policy

Any Staff member presently responsible for a Student will be considered responsible for ensuring Student adherence to this Policy. Staff members have the authority to challenge any Student on any activity they feel is not in accordance with this Policy and remove the Student from the facilities for a period of time if they feel this is necessary to ensure the security and efficiency of the Network.

Students are still responsible for their own adherence at all times and are solely accountable for their actions. The actions of others will not be taken as a mitigating factor, nor will claimed ignorance of this Policy.

55. Potential Repercussions for Contraventions of this Policy

This Policy forms the basis for potential Disciplinary Action and sanctions can range from verbal warnings to exclusion in accordance with existing disciplinary procedures.

Other sanctions that may be taken that are specific to this policy include the withdrawal of privileges such as email, printing, internet or network access for a specified period of time or indefinitely, depending on the severity of the transgression. The severity of the transgression and the repetition of offences will be taken into account when deciding the appropriate response.

56. Exceptions to the Inappropriate Materials and Misuse Clauses

Where explicitly directed to by a member of Staff, a Student may access a site that would otherwise fall into the definitions of Inappropriate Material as defined in Appendix 1, Section 37 in order to complete work set in pursuit of a School Activity. This explicit permission can extend outside of lessons where it is necessary for the completion of homework or extra-curricular activities, but the Student's usage must not fall outside of the bounds explicitly allowed by the Staff member setting the task.

57. Definition of Reasonable Personal Use

Allowance for reasonable personal use is made in sections 6 and 18 of the main Policy, where "reasonable personal use" is defined as use that "does not interfere with the education of the Student Body". The practical implication of this for Students is that any time a Student is using the Network for any use that is not expressly related to a School Activity, they must give up such equipment as is in use for another Student that requires said equipment for work related to a School Activity at the request of said Student.

Such personal use may also not have an impact on the operation of the Network as a whole. Due to the limited bandwidth available to the School and the number of Students with access to the Internet, Students are therefore banned from streaming any audio or visual content from the Internet unless explicitly authorised by a Staff member for a specific School Activity. This includes the use of any website where such content is available (e.g. YouTube, BBC iPlayer) or any software that streams content (e.g. Spotify).

58. Security, Honesty & Privacy on the Network

Students may make use (in whole or part) of material prepared by a Staff member where directed to by the original author or another member of Staff who has permission from the original author. Any use without permission is considered plagiarism.

Students may not make use of any other Student's work in part or whole and any such attempts will be treated as plagiarism.

59. Dissemination of Personal Details

Students may reveal such personal details as instructed by a member of Staff in the pursuance of a School Activity; for example, contacting potential employers for work experience, or writing a letter to an exchange student.

60. The Use of Messaging Services including Chat Rooms

Exception is made for such services as are automatically connected to a school account e.g. Microsoft Teams. Any such services should only be used as directed by a member of staff and in a manner explicitly pursuant to education e.g. a teacher may direct students to use Teams to discuss a project, but students should not otherwise use Teams for socialising and time-wasting.

61. Permission to Use Personal Equipment

Students may only bring personal electronic equipment on site where a teacher has given written permission to ICT Support on behalf of a student and confirmed that the equipment is necessary for educational purposes.

Key Stage 5 students may bring personal equipment on site for use with the Guest wireless network, which allows access to the internet only and not any internal services (including printing). As per section 34 of the main policy, students are wholly responsible for their own equipment, and the school is not liable for any damage or harm that may arise from use on the network (e.g. a virus infection spread through the Guest network, which by its nature is outside the control of the IT Support department).

62. Mass Communications

Students are restricted from emailing Distribution Lists (e.g. AA All Students) and may not seek to circumvent the technical restrictions in order to email large groups of students at once e.g. whole year groups. Any emails that require the attention of a large body of students (e.g. messages regarding the organisation of a school-sanctioned event, such as a prom) should be discussed with the appropriate Head of Year and sent via them.

Appendix 3B - ICT Acceptable Usage Policy

Summary of Acceptable Use Policy - Students

This document is intended as a readable summary of the KGGS AUP. You should still familiarise yourself with the full document as you are agreeing to abide by the full policy.

All Students agree:

- **To keep their account secure by not sharing their password or logon and by not leaving any computer they are logged onto unattended and open.**
- That the network exists for learning, and not to disrupt their own or anyone else's learning through inappropriate use of the network. This includes giving up machines for students who need to work if you are not working yourself.
- Not to use, view, print, store or send anything that is: pornographic, criminal, illegal, racist, sexist or bullying in any way, unless instructed to by a member of staff (for example, in a lesson on drugs). A complete list can be found in the full policy.
- Not to allow any security risks to either the network or themselves, either from malicious software (e.g. viruses) or malicious websites (e.g. phishing scams).
- Not to (attempt to) circumvent any security, filtering or monitoring systems on the Network in any way.
- Not to install any new or unauthorised software or hardware.
- To only use copyrighted material within the bounds of the school/county licensing.
- Not to stream any video or audio content unless told to by a member of staff.
- Not to save any video, music or picture files unless necessary for work.
- Not to post any comment or material online that is related to the school or any members of staff or any students, including photos/videos/audio of staff or students.
- Not to tell anyone any of their personal details online.
- Not to use any online chat facility (including Instant Messengers or chat rooms hosted on web sites) or use other online communications (such as forums) or access any personal e-mail accounts when in school.
- That any personal equipment brought on site may only be used by the owner and cannot be shared; it must also not endanger the network in any way.
- To abide by the Data Protection Act 2018 for all data collected on any member of the school for any purpose, including school projects and research.
- To report anyone they think is breaking this policy to a member of staff.
- To consent to the processing & transfer of their data where relevant in accordance with the requirements of the School, the Department of Education and the LEA.

All Students are aware that:

- Activity on the network and on the Internet is monitored for the safety of all users.
- All files and emails are accessible by ICT Support. Teachers can view files.
- They are responsible for their own actions.
- Anybody breaking this policy may be blocked from the network and further action taken by the Headteacher.

I have read and understood this policy:

Signed: _____ Date: _____

Printed Name: _____ Form: _____



Parents/Guardians Signature: _____ Date: _____

Printed Name: _____ Relationship: _____

Confidential Once Signed

Kesteven & Grantham Girls' School

(this page left intentionally blank)

ICT Acceptable Usage Policy

Appendix 4

Current Licensing Agreements for Copyrighted Material



Kesteven and Grantham Girls' School

Appendix 4 – Current Licensing Agreements for Copyrighted Material

Section 14 of the main Policy states that *“Users agree not to broadcast or use copyrighted films, music, television programming, images or text except where the School is specifically licensed for the intended material and purpose”*. This Appendix will therefore lay out the specific licenses that the School and LEA hold and the usage therefore allowed by the terms of these licenses. Please note that this document is subject to change at the whim of third-parties i.e. the licensing bodies and the School cannot be held responsible for changes made to terms that Users have previously relied on.

The sections below are not an exhaustive description of each license but are intended to serve as a useful summary of the terms of each license. For a fuller description of the license and exactly what is defined in these licenses, please visit the website link provided in each section.

63. Public Video Screening License (PVSL)

Held by: Department for Education

Website: http://www.filmbank.co.uk/licences/public_video_screening.asp

The PVSL license allows the School to show films for entertainment purposes during and outside of school hours, including extra-curricular film clubs. This is limited to non-paying audiences, including offering refreshments for sale at an event where a film is playing. Please note that a current PRS for Music license is required in order to play a film with a soundtrack, as the music is covered under a separate license. Please see section 64 of this Appendix for more details.

The PVSL licence covers a subset of the studios/distributors active in the market. An up to date list of these studios/distributors can be found on the FilmBank website at <http://www.filmbank.co.uk/>.

64. Performing Rights Society (PRS) for Music License

Held by: Department for Education

Website: http://www.cefm.co.uk/licensing/prs_ee/index.htm

The PRS for Music License allows the School to use music in any extra-curricular public performance. The PRS represents the composers, songwriters and publishers of music. Please note that a separate organisation represents the rights of the record companies that manufacture pre-recorded media; see section 65 of this Appendix for details of the PPL License.

In conjunction with the PVSL license detailed in section 61 of this Appendix, this allows films with a soundtrack to be played with the sound at an audible level.

Any commercial use of music (e.g. selling a DVD recording of a show in which music was used, such as a dance production) may need to be licensed directly by PRS for Music.

65. Phonographic Performance Limited (PPL) License

Held by: Department for Education

Website: http://www.cefm.co.uk/licensing/ppl_ee/index.htm

The PPL License allows the School to use pre-recorded music in conjunction with the PRS for Music license detailed in section 64 of this Appendix.

66. Educational Recording Agency (ERA) License

Held by: Department for Education

Website: <http://www.era.org.uk/>

The ERA scheme permits recordings of broadcasts to be made for non-commercial educational use. A 'broadcast' is defined as a transmission for simultaneous and lawful reception by members of the public i.e. it is not encrypted or encoded and is for general reception, unlike pay per view services. The ERA Licence therefore covers scheduled free to air broadcasts on:

- BBC television and radio
- ITV Network services (including ITV2 and ITV3)
- Channel Four, E4, More 4 and Film 4
- Five Television
- S4C

It also applies to any other licensed broadcast services. These cover both radio and television services.

Recordings may be made available to students over the internet so long as access is restricted by login such that the material is not publicly available but accessible only by students, for example made available through remote file access.

Please note that "on-demand" services are not considered to be broadcasts under the Act and are therefore not covered by this license. Open University programs are also covered by a separate license that does not currently cover the School.

67. Copyright Licensing Agency (CLA) License

Held by: Department for Education

Website: <http://www.cla.co.uk/>

The Copyright Licensing Agency Ltd licenses the photocopying and scanning of extracts from books, journals and magazines for the purpose of teaching, training or information on behalf publishers, authors and visual creators. Use of digital copies with digital whiteboards, VLE's or PowerPoint presentations is also covered.

68. Motion Picture Licensing Company (MPLC)

Held by: Department for Education

Website: <http://www.themplc.co.uk/>

The Motion Picture Licensing Company (MPLC) Umbrella Licence allows the School to show films for entertainment purposes during and outside of school hours, including extra-curricular film clubs. This is limited to non-paying audiences, including offering refreshments for sale at an event where a film is playing.

The MPLC licence covers a subset of the studios/distributors active in the market. An up to date list of these studios/distributors can be found on the MPLC website at <http://www.themplc.co.uk/page/producer-list>.

69. Schools Printed Music License (SPML)

Held by: Department for Education

Website: <http://www.cla.co.uk/>

Printed Music Licensing Ltd licenses the photocopying, scanning, and reproduction by score writing software, of printed music owned by the school. Scans of music can be made available on shared areas. Musical works can be adapted for performance by the instrumental and vocal resources available to the school.

70. Christian Copyright Licensing International (CCLI)

Held by: Department for Education

Website: <http://uk.ccli.com/>

The CCLI Collective Worship License allows the school to project song words, reproduce them in song sheets, photocopy music from song books or music publications in pursuit of collective worship.

Configuration History

Version:	Date:	Authors	Contributors
2.1	March 2010	Matthew Dovey (Network Manager) Piers Mayfield (Head of Curriculum ICT)	Ken Billington (School Governor)
2.2	June 2010	Matthew Dovey (Network Manager) Piers Mayfield (Head of Curriculum ICT)	Ken Billington (School Governor)
2.3	July 2010	Matthew Dovey (Network Manager) Piers Mayfield (Head of Curriculum ICT)	Ken Billington (School Governor)
3.0	June 2012	Matthew Dovey (Network Manager)	Piers Mayfield (Head of Curriculum ICT) Ken Billington (School Governor)
3.1	June 2014	Matthew Dovey (Network Manager)	
4.0	June 2016	Matthew Dovey (Network Manager) David Scott (Headteacher)	
5.0	June 2018	Matthew Dovey (Network Manager)	
6.0	September 2020	Matthew Dovey (Network Manager)	
6.1	June 2022	Matthew Dovey (Network Manager)	

Audit trail of change

Version:	Date	Reason for change
2.1	March 2010	Modified structure of document;
2.2	June 2010	Modified structure of document;
2.3	July 2010	Modified structure of document;
3.0	June 2012	Scheduled review of document;
3.1	June 2014	Scheduled review of document;
4.0	June 2016	Scheduled review of document;
5.0	June 2018	Scheduled review of document.
6.0	September 2020	Scheduled review of document;
6.1	June 2022	Scheduled review of document

Authorisation

Name	Date	Signature
Mr N Boddington	June 2022	