Keswick School

UNCONTROLLED if COPIED or PRINTED

Keswick School is not liable for the contents of this document

ONLINE SAFETY (KS/C&P/034)
(INCLUDING ACCEPTABLE USE OF IT)

Committee Responsible:	Pupil Progress and Pastoral Welfare
Lead Officer:	Headteacher
Date of Review:	October 2022
Date to be Reviewed:	October 2025
Signed: **Date:**	

Head teacher: S. Jackson, M.A. (Oxon), M.Ed., FRSA
Keswick School Multi Academy Trust
a company limited by guarantee
Registered in England: Company Number: 07664297
Registered Office: Vicarage Hill, Keswick, Cumbria, CA12 5QB
Tel. 017687 72605
Email: admin@keswick.cumbria.sch.uk
Web: http://www.keswick.cumbria.sch.uk

ONLINE SAFETY POLICY

REVIEW SHEET

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date.

Version Number	Version Description	Date of Revision
1	Original Policy	June 2014
2	Policy Review	November 2015
3	Policy Review	February 2016
4	Policy Review	November 2019
5	Policy Review	October 2022

ONLINE SAFETY POLICY

Contents

ONLINE SAFETY POLICY

1.0 INTRODUCTION AND AIMS

1.1 The use of IT in school and at home has been shown to raise educational standards and promote pupil achievement. The purpose of the online safety policy is to ensure safe and appropriate IT use in school and at home. A wide range of legislation is relevant to this policy including the Malicious Communications Act, The Data Protection Act and the Computer Misuse Act (see Appendix 3).

1.2 Some of the risks and dangers associated with IT include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- The risk of being targeted by extremists in order to promote and encourage radicalisation
- The risk of being targeted by those involved in child sexual exploitation
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning.

1.3 Many of these risks reflect situations on internet based social networks. It is therefore essential that this online safety policy is read and used in conjunction with the following school policies:

- Anti-Bullying (KS/PP&PW/045)
- Behaviour (KS/PP&PW/044)
- Child Protection and Safeguarding (KS/PP&PW/040)
- Code of Conduct (KS/GEN/039)
- Data Protection (KS/PP&PW/062)
- BYOD (KS/PP&PW/065)
- Tackling Radicalisation and Extremism Policy (KS/PP&PW/080)
- Sexting Policy (KS/PP&PW/078)

1.4 It's impossible to eliminate the risks outlined above. It's therefore essential, through good educational provision, to build pupils' resilience to these risks so they have the confidence and skills to deal with them. The school provides the necessary safeguards on its own network to manage and reduce the risks.

2.0 ROLES AND RESPONSIBILITIES

2.1 The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online-safety related incidents.

2.2 The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can be taken over issues covered in the Behaviour Policy (KS/PP&PW/044).

2.3 Keswick School will where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

2.4 **Head teacher / Senior Leadership Team (SLT)**

The Head teacher will:

- Oversee the safety (including online) of all members of the school community.
- Take overall responsibility for data and data security.
- Ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements
- Ensure that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- Ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- Receive regular updates from the Online Safety Coordinator
- Be aware of the procedures to be followed in the event of a serious online safety incident or an allegation being made against a member of staff or volunteer (The procedures for dealing with allegations against staff or volunteers can be found within the school Child Protection and Safeguarding Policy (KS/PP&PW/040).

2.5 **Online Safety Governor: Emily Hudson**

- Regular monitoring of online safety incidents.
- Report to the Pupil Progress and Pastoral Welfare committee.

2.6 **Online Safety Coordinator: Tania Gibbin (Deputy Head: Pastoral)**

- Day to day responsibility for online safety.
- Liaise with staff, IT technicians, online safety governor and SLT on all issues related to online safety.
- Ensuring that all staff are aware of the procedures to follow in the event of an online safety incident taking place.
- Providing training and advice for staff.
- Receiving reports of online safety incidents and create a log of incidents to inform future online safety planning.
- Co-ordinate and review the online safety education programme in school.

2.7 **IT Network Manager: Steven Waning**

- Report any online safety related issues that arise to the Online Safety Co-ordinator.
- Ensure that users may only access the school's networks through an authorised and properly enforced Data Protection Policy (KS/PREM&BLDGS/062).
- Ensure that the school's IT infrastructure is secure and is not open to misuse or malicious attack e.g. keeping virus protection up to date.
- That the school meets the online safety technical requirements outlined in the school Acceptable Use Policy (AUP) and any relevant Local Authority Online Safety Policy and guidance;
- The school's policy on web filtering, is applied and updated on a regular basis;
- Ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices;
- Keep up to date with technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- That the use of the network/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Co-ordinator/Head teacher/Head of IT/Head of Year for investigation/action/sanction;
- Ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster and in order to complement the business continuity process;
- Keep up-to-date documentation of the school's online security and technical procedures;
- The IT network is secure and meets online safety requirements;
- Attends training, as necessary, on up-dating technical online safety processes and procedures;
- To monitor and maintain the online safety monitoring software installed on all curriculum computers and to report any issues to the Online Safety Coordinator.

2.8 **Teaching & Associate Staff**

- Read, agree and sign the staff Acceptable Use Policy (Appendix 1).
- Have up-to-date awareness of online safety matters, policy and practices.
- Embed online safety issues into the curriculum and other school activities.
- Ensure pupils understand and follow the pupil Acceptable Use Policy (Appendix 2).
- Ensure pupils understand the need to avoid plagiarism and uphold copyright regulations.
- Monitor IT activity in lessons, extracurricular and extended school activities.
- Check internet sites are suitable, where possible, and that processes are in place to deal with unsuitable material found through internet searches.

2.9 **Pupils**

- Read, agree and sign the pupil Acceptable Use Policy (Appendix 2) - part of the Home/School agreement. Boarders have a separate policy which must be signed (Appendix 3).
- Report abuse, misuse or access to inappropriate materials.
- Adopt good online safety practice out of school.
- Understand that this online safety policy covers their actions out of school, if related to their membership of the school.

2.10 **Pupils with Additional Needs**

2.10.1 The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' online safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

2.10.2 Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety.

2.10.3 Internet activities need to be planned and well managed for these pupils.

2.11 **Parents**

- Read and agree to the pupil Acceptable Use Policy (Appendix 2) - part of the Home/School agreement.
- Ensure that their child understands the need to use IT in an appropriate way.
- Be a positive role model in their use of IT at home.
- Monitor the use of social networking and gaming sites and alert the relevant Form Head if they have concerns.
- Ensure that their child does not engage in any online behaviour that could have a detrimental impact on their membership of the school.

3.0 EDUCATION PROGRAMME

3.1 Online safety is covered in the pastoral and assembly programme and is regularly revisited in IT/ Personal Development and computing lessons and across the curriculum – this programme covers the safe and responsible use of IT both within and outside of school.

Keswick School:

- Has a clear online safety education programme as part of the Computing curriculum/Personal Development curriculum. This covers the teaching of a range of skills and behaviours which are appropriate to the age and experience of the pupils concerned and include those to:
  - develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - know how to narrow down or refine a search;
  - [for older pupils] understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - understand acceptable behaviour when using an online environment/e-mail, i.e. be polite, no bad or abusive language or other inappropriate behaviour;
  - keeping personal information private;
  - understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - understand why they must not post pictures or videos of others without their permission;
  - know not to download any files – such as music files – without permission;
  - have strategies for dealing with receipt of inappropriate materials;
  - [for older pupils] understand why and how some people will 'groom' young people for sexual reasons;
  - understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying;
  - know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign/will be displayed when a pupil logs on to the school network;
- ensures staff will model safe and responsible behaviour in their own use of technology during lessons;
- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online, online gaming/gambling etc.

4.0 COPYRIGHT

4.1 Pupils and staff should be aware of and uphold copyright regulations. Pupils are taught to do this in the following ways:

- Develop a good understanding of IT research skills and the need to avoid plagiarism.
- Acknowledge the source of information used.
- If using a search engine for images, open the selected image and go to it's website to check for copyright.
- To be critically aware of content accessed on-line and the need to validate accuracy.

5.0 TRAINING

- Online safety CPD is available to all staff.
- All new staff receive online safety training as part of the safeguarding CPD throughout the year.
- Online Safety Coordinator to receive regular updates/training and review guidance documents.
- Governors are invited to take part in online safety training and awareness sessions.

6.0 E-MAIL

- Digital communication with pupils (e-mail, blogs etc.) should be on a professional level only.
- E-mails should only be sent and received via the school's web-based system - under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt.

7.0 SOCIAL NETWORKING

- Pupils are not allowed on social networking sites at school.
- At home it is the parental responsibility (parents should be aware that it is contravening the sites regulations for children under the age of 13 to be on certain social networking sites).
- Staff users must not reveal the names of staff, pupils, parents or any other member of the school community on any social networking site.
- Pupils and parents should be aware that the school will investigate the misuse of social networking if it impacts on the well-being of other students or members of the school community.

- If inappropriate comments are placed on social networking sites about the school or school staff then advice will be sought from the relevant agencies, including the police if necessary.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding a pupil's use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents, particularly when concerning the underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and outlined in the school Staff Acceptable Use Policy

8.0 DIGITAL IMAGES

- The school record of parental permissions must be adhered to when taking images of our pupils - a list can be obtained from the administration office.
- Images must not be taken using privately owned equipment without the prior permission of the Head teacher.
- Where permission is granted the images should be transferred to school network and deleted from privately owned equipment at the earliest opportunity.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work;
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents.

9.0 REMOVABLE DATA STORAGE DEVICES

- Personal or confidential data must only be downloaded onto an encrypted or password protected data storage device and practices must fully comply with the Data protection policy (KS/PP&PW/062).
- All files downloaded from the Internet, received via e-mail or brought into school on a data storage device must be checked for viruses using school anti-virus software before being opened or copied onto the IT network.

10.0 INTERNET USE

- Staff will preview any recommended websites before use.
- If Internet research is set for homework, specific sites that have previously been checked may be suggested - parents are advised to supervise any further research.
- Staff must actively monitor what pupils are viewing on the internet in lessons.
- Pupils must be made aware that all internet use at school is tracked and logged.
- The online safety co-ordinator, IT Network manager and SLT have access to internet logs.

11.0 PASSWORDS

- Passwords or encryption keys should not be recorded on paper or in an unprotected file.
- Good practice is for staff to change their passwords at least every 3 months.
- Users should not use the same password on multiple IT systems.
- Pupils must only let school staff know their in-school passwords and inform staff immediately if passwords are used by someone else or forgotten. Passwords are set by the IT technicians.

12.0 USE OF PERSONAL IT DEVICE

- The school is actively engaged on a Bring Your Own Device (BYOD) programme.
- The BYOD policy and agreement (KS/PP&PW/065) sets out the terms and conditions for pupils to use their own devices to access the internet and teaching resources through the school's Wi-Fi during the school day.

12.1 **Pupils use of personal devices:**

- Students can bring mobile phones or similar devices into school on the understanding that mobile phones remain switched off and in bags throughout the school day. Students are <u>not</u> permitted to have mobile phones out during the school day.
- Staff will confiscate any electronic device being used inappropriately on the premises such as mobile phones, laptop, notebooks, tablets etc. Confiscated devices will be kept by the Head teacher's PA or the IT Technicians for 1 week. Parents are given an option to collect them from school (see Section 8.0 of the Behaviour Policy (KS/PP&PW/044).
- Phones and devices **<u>must not</u>** be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents they will be allowed to use a school phone at Pupil Reception. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

12.2 **Staff use of personal devices:**

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the school in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents is required.
- Mobile phones and personally owned devices will be switched off or switched to 'silent' mode; Bluetooth communication should be "hidden" or switched off and mobile phones or personally owned devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Where members of staff are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- If a member of staff breaches the school policy then disciplinary action may be taken.

13.0 USE OF SCHOOL IT DEVICE

- No software packages should be installed on school IT equipment without permission of the IT Network Manager.
- Personal or confidential data should not be stored on local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- Staff must ensure any screens are locked before moving away from a computer during the normal working day to protect personal or confidential data and to prevent unauthorised access.

14.0 MONITORING

- All use of school internet access is logged.
- Internet logs are randomly but regularly monitored.
- If inappropriate use is detected it will be followed up by the online safety co-ordinator, Heads of Year/Department or SLT depending on the severity of the incident.
- IT Rooms are monitored by CCTV.
- Computers are monitored by e-safety software and in real time.

15.0 INCIDENT REPORTING

- Online safety incidents involving a pupil must immediately be reported to the online safety co-ordinator via the Online Incident Referral Form (see Appendix 5).
- Online safety incidents involving a member of staff must immediately be reported to the Head teacher.

16.0 RESPONDING TO INCIDENTS OF MISUSE

16.1 It is hoped that all members of the school community will be responsible users of IT. However, if infringements do occur they will be dealt with swiftly.

16.2 If any apparent or actual misuse appears to involve illegal activity this must be reported immediately to the Head teacher. Such matters will then be reported to the police.

16.3 Where misuse is not deemed to have been illegal it will be dealt with under the terms set out in the Behaviour policy (KS/PP&PW/044) for pupils and the Code of Conduct (KS/GEN/039) and Disciplinary policy (KS/PER/011) for staff.

17.0 COMPLAINTS

17.1 Parents, teachers and pupils should know how to use the school's complaints procedure (KS/PER/021). The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. Online safety incidents may have an impact on pupils; staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

17.2 A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's Behaviour Policy (KS/PP&PW/044).

17.3 Potential child protection or illegal issues must be referred to the school Designated Safeguarding Lead. Advice on dealing with illegal use can, when deemed necessary, be discussed with the Police or Cumbria Safeguarding Hub.

17.4 The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable materials will never appear on a school computer or mobile device. Neither the school staff nor the Governing Body/Board of Directors can accept liability for material accessed, or any consequences of Internet access.

17.5 Sanctions available include (this is not an exclusive list):

- Interview/counselling by class teacher/Head of Year/online safety coordinator/Head teacher;
- Informing parents;
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework;
- Referral to the Police.

17.6 Our e-safety coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

- Parents and pupils will need to work in partnership with the school to resolve issues.
- 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 or which may bring the school into disrepute.

Appendix 1

Acceptable IT Use - Staff

The school's IT system is made available to staff to enhance their teaching. This acceptable use policy (AUP) has been drawn up to protect all parties - the pupils, staff and the school. The school reserves the right to examine or delete any files that may be held on its IT system; users should not expect that files or e-mail stored on servers or disks will always be private. All e-mail correspondence and internet sites accessed are audited and inspected periodically.

Staff requesting access to the school's IT system must sign a copy of this AUP and return it to the IT office. By signing a copy of this AUP you are indicating that you have read and understand the online safety policy and are consenting to the school's IT monitoring practices.

The IT system in Keswick School may not be used for any of the following:

- Sending or displaying offensive, abusive or threatening messages or pictures
- Accessing undesirable materials. Examples of undesirable material are not restrictive but include the following:
  - Written or photographic material depicting sexual behaviour
  - Written or photographic material depicting violent or threatening behaviour
  - Written or photographic material depicting use of illegal or disreputable substances
  - Written or photographic material depicting any illegal practice
  - Threatening, obscene or abusive language
  - Photographs of other individuals in school taken and stored without their permission
  - Material that could be considered to be of an extremist nature or could contribute to radicalisation of young people
- Violating copyright laws
- Using another's password
- Trespassing in another's folder, work or files
- Intentionally wasting limited resources (including time)
- Using school IT equipment for commercial purposes
- Using school IT equipment for unauthorised personal purposes
- Using school IT equipment for any purpose that would bring the name of the school into disrepute
- Interfering with the functioning of any school IT equipment, including the school network, the service provider's network, or any other network that can be accessed in school
- Causing damage to school IT equipment through intentional or negligent abuse
- Attempting to gain unauthorised access to any IT system, data or resource
- Accessing material or information that may be related to extremist views or related to radicalisation of students or others
- Using any Webcams in areas where pupils are or without permission of a member of SLT.

Violations of these rules may result in:

- A temporary or permanent ban in the use of the school's IT system;
- Additional disciplinary action if this is thought necessary;
- The police or other agencies may be involved if this is felt appropriate.

Appendix 2

Acceptable IT Use - Pupils

For my own personal safety:

- I understand that the school will monitor my use of IT systems, email and other digital communications.
- I will not share my password, nor will I try to use any other person's username and password.
- I will be aware of "inappropriate contacts", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will make staff aware if any other pupils are accessing material or information that may be related to extremist views or I am concerned that potential radicalisation is taking place.
- I must not use any Webcams in areas where other pupils are or without permission of a member of staff.

I understand that everyone has equal rights to use IT as a resource and:

- I understand that the school IT system is intended for educational use.
- I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school IT system for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission to do so.
- I will not use any personal Wi-Fi hot spots to gain unrestricted access to the internet.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of its IT system:

- I will only use my personal external devices (USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to illegal or inappropriate materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use chat and social networking sites.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this home-school agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and, in the event of illegal activities, involvement of the police.

Appendix 3

Acceptable Use of IT - Lairthwaite Boarding House

Aim

- To ensure that boarders will be responsible IT users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- To ensure that school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Agreement

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.

For my personal safety:

- I understand that the school will monitor my use of the IT systems, email and other digital communications.
- I will not share my password, nor will I try to use any other person's username and password or equipment.
- I will be aware of "inappropriate contacts", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and will take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will make staff aware if any other Boarders are accessing material or information that may be related to extremist views or I am concerned that potential radicalisation is taking place.
- I must not use any Webcams in areas where other borders are, if I wish to use a Webcam it must be in one of the areas designated by a member of staff.

Everyone has an equal right to use technology and:

- I understand that the school IT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school network for on-line gambling, file sharing, or video broadcasting.
- I will not use the school network for imposing my views on others, including encouraging others to access inappropriate material.
- I will not use any personal Wi-Fi hot spots to gain unrestricted access to the internet.

Appendix 4

LEGAL FRAMEWORK

Keeping Children Safe in Education, September 2022

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.
Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Communications Act 2003 (Section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on

conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

The Computer Misuse Act 1990 (sections 1 - 3)

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

General Data Protection Regulations 2018

This law regulates how companies protect personal data. GDPR aims to create more consistent protection of consumer and personal data. GDPR mandates a baseline set of standards for companies that handle data to better safeguard the processing and movement of personal data. Some of the key privacy and data protection requirements of the GDPR include:

- Requiring the consent of subjects for data processing
- Anonymizing collected data to protect privacy
- Providing data breach notifications
- Safely handling the transfer of data
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the

result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Public Order Act 1986 (sections 17 — 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964 and update in 2019
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Investigatory Powers Act 2016
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Criminal Justice and Immigration Act 2008
Section 63 offence to possess "extreme pornographic image"
63 (6) must be "grossly offensive, disgusting or otherwise obscene"
63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyber-bullying/ Bullying:

- Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/antibullying policy.

Telecommunications Act 1996
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial.
- The right to respect for private and family life, home and correspondence.
- Freedom of thought, conscience and religion.
- Freedom of expression.
- Freedom of assembly.
- Prohibition of discrimination.
- The right to education.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Appendix 5

ONLINE SAFETY INCIDENT REFERRAL FORM

Please complete the following information if you need to report an online safety incident – **this should be returned to TG directly.** Everyday concerns should still be addressed to Form Tutor or Head of Year as appropriate.

Name of Pupil	Form

Nature of Referral/Concern	Please Tick
• **Pupils have brought inappropriate material to school – on a memory stick or their own device**	
• **Pupils have expressed concern about messages they have received in school**	
• **Pupils report incidents of cyber-bullying**	
• **Pupils disclose information about inappropriate images of themselves (or others) being distributed in school**	
• **Pupils disclose information about people who have been contacting them and they are concerned about this**	
• **Attempts to access inappropriate material in class/school**	
• **Parental contact regarding online safety (detail below)**	
• **Comments made in class – orally or in written work**	
• **Any other comments/concerns**	

Name of Member of Staff/Subject	
Date	