Keswick School

UNCONTROLLED if COPIED or PRINTED

Keswick School is not liable for the contents of this document

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

Committee Responsible:	Pupil Progress and Pastoral Welfare
Lead Officer:	Headteacher
Date of Review:	January 2024
Date to be Reviewed:	January 2027
Signed: **Date:**	

Head teacher: S. Jackson, M.A. (Oxon), M.Ed.,

Keswick School Multi Academy Trust
a company limited by guarantee
Registered in England: Company Number: 07664297
Registered Office: Vicarage Hill, Keswick, Cumbria, CA12

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
6	Policy Review – updated roles and responsibilities, inclusion of use of private online tuition in boarding and an update on filtering and monitoring included as a new appendix.	January 2024

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 gambling/gaming sites;
- 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, a copy of these polices are available on the school website or by contacting the school:

- Behaviour (KSMAT/STAT/044) including Anti-Bullying
- Child Protection and Safeguarding (KSMAT/STAT/040)
- Code of Conduct (KSMAT/STAT/039)
- Data Protection (KSMAT/STAT/023)
- BYOD (KS/CUR/065)
- Preventing and Tackling Extremism and Radicalisation Policy (KS/P&B/080)
- Sexting Policy (KS/P&B/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:

- Take overall responsibility for data and data security;
- oversee the safety (including online) of all members of the school community and ensure that policies and procedures are followed by staff and other adults working in the school;
- liaise with the DSL/IT Network Manager on all online-safety issues which might arise;
- take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling;
- work with the Data Protection Officer (**Ruth Lawler**), DSL and Governors to ensure a Data Protection Act 2018 compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information;
- ensure the school implements and makes effective use of appropriate IT systems and services including filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles;
- liaise with the Governors in order to achieve their obligations in meeting the DfE digital and technology standards, particularly as they relate to cyber security and filtering and monitoring and ensure the Governors are regularly updated on progress towards the standards;
- undertake an annual review of the school's approach to online safety and an associated risk assessment that considers the risks children face;
- ensure **all** staff receive training on induction to carry out their child protection and online safety roles (which should include the procedures and processes in place to manage filtering and monitoring and how to escalate concerns when identified);
- make staff aware of the procedures to be followed in the event of a serious online safety incident or an allegation 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);
- formulate the school's Cyber security resilience strategy and Cyber response plan in liaison with the DPO, DSL, IT Network Manager, Online Safety Governor and other third-party providers;
- encourage parents/carers to provide age-appropriate supervision for children in their care using the internet including by the use of internet filters which should be used to block malicious websites. Information for parents/carers will be regularly updated and published on the school website and via newsletters and other publications.

2.4 **Senior Leadership Team (SLT) digital lead – Jill Wilson**

- encouraging and supporting the use of digital technology across the school;
- have strategic oversight of all digital technology and how it fits with their development plan;
- create and manage the digital technology strategy led by the needs of staff and students, not the technology itself;

- the delivery of the digital technology strategy based on teaching and learning outcomes and organisational needs;
- identifying and acting on digital technology training needs for staff and students;
- help all staff to embed digital technology that meets staff and student needs;
- reviewing the effectiveness of IT support to inform decision making and taking action, when necessary;
- liaise with SLT, IT Network Manager, DSL, DPO and curriculum leads about matter concerning digital technology and how this fits into the development plan.

2.5 **Online Safety Governor: Emily Wilson**

- ensure a member of the School Leadership Team (SLT) is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety and an understanding of the filtering and monitoring systems and processes in place);
- ensure other roles and responsibilities are appropriately allocated to staff and third parties, e.g. external service providers, in order to meet the DfE Digital and technology standards;
- ensure that systems are in place to meet the requirements of the DfE Cyber security standards, including a Cyber security and resilience strategy and a Cyber response plan;
- ensure that the school follows all current online safety advice (including that for online filtering and monitoring) to keep both pupils and staff safe;
- have regular reviews with the Designated Safeguarding Lead (DSL) and IT Network Manager, and ensure Governors receive information about online safety incidents, monitoring reports, filtering and monitoring change logs etc.
- ensure that all staff undertake regular updated safeguarding training, including online safety training, in line with advice from the Local Safeguarding Children's Partnerships (LSCP);
- ensure Governors and Trustees receive appropriate training on online safety which includes an understanding of filtering and monitoring in relation to school owned IT devices;
- work with the DPO, DSL, IT Network Manager and Head teacher to ensure a data protection compliant framework for storing data and data protection processes which support careful and legal sharing of information;
- ensure pupils are taught how to keep themselves safe, including online as part of providing a broad and balanced curriculum.
- support the school in encouraging parents and the wider community to become engaged in online safety activities.

2.6 **Online Safety Coordinator: Wendy Lightfoot (Deputy Head: Pastoral)**

- take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place);
- be the first point of contact for any concerns the wider staff and other adults working in the school may have in relation to child protection and online safety harmful behaviour e.g. sharing nude and/or semi-nude images and/or videos/online challenges or hoaxes;
- understand the unique risks associated with online safety (including an understanding of the filtering and monitoring systems and processes in place in the school) and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school and to support other adults in doing so;
- oversee and discuss 'appropriate filtering and monitoring' with Governors in order to meet the DfE Filtering and monitoring standards (both physical and technical) and ensure staff are aware of its necessity;

- liaise with staff, DPO, IT Network Manager, Online Safety Governor and SLT on all issues related to online safety;
- ensure that all staff are aware of the procedures to follow in the event of an online safety incident taking place;
- provide training and advice for staff;
- receive 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**

- all as listed in the 'Teaching & Associate Staff' section below;
- supporting Governors and SLT in achieving the DfE digital and technology standards;
- supporting SLT in the formulation of a Cyber Security resilience strategy and appropriate Cyber response plan as outlined in the DfE Cyber security standards;
- reporting any online safety related issues that arise through external monitoring reports, to the DSL in the first instance;
- keeping up to date with the school's Online safety Policy and technical information to effectively carryout their online safety role and to inform and update others as relevant;
- working closely with the DSL/DPO to ensure that school systems and networks reflect school Policy;
- ensuring that the above stakeholders understand the terms of existing services and how any changes to these systems (especially in terms of access to personal and sensitive records/data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.) might affect the system functions and safety online;
- supporting and providing advice on the implementation of 'appropriate filtering and monitoring' in order to meet the school's obligations outlined in the DfE Filtering and Monitoring standards;
- ensuring that users may only access the school's networks through an authorised and properly enforced password protection procedures, in which passwords are regularly changed;
- ensuring 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;
- ensuring that access controls/encryption exist to protect personal and sensitive information held on school-owned devices;
- monitoring the use of the network/email and that any misuse/attempted misuse is reported to the DSL/Head teacher/Head of IT/Head of Year for investigation in line with school policy;
- ensuring that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a cyber-attack or other disaster and to complement the business continuity process and cyber response plan;
- maintaining up-to-date documentation of the school's online security and technical procedures;
- reporting online safety issues that come to their attention in line with school policy.

2.8 **Teaching & Associate Staff**

- read, understand, and help promote the school's Online Safety Policy and procedures in conjunction with the Child Protection and other related school policies and procedures;
- read, sign, and follow the school Staff Acceptable Use Agreement (Appendix 1) and the staff Code of Conduct;
- be aware of online safety issues related to the use of mobile technology e.g. phones, cameras, smart watches and other hand-held devices and follow school procedures in relation to these devices;

- ensure the security of their username and password for the school system, not allow other users to access the systems using their log on details and immediately report any suspicion or evidence that there has been a breach of security;
- understand the different roles and responsibilities for the filtering and monitoring of online systems and expectations of them in their role, including for their own online activities on any device using the school network or on school-owned devices using any network;
- record online safety incidents in the same way as any child protection incident and report incidents to the DSL in accordance with school procedures;
- notify the DSL if policy does not reflect practice in the school and follow escalation procedures if concerns are not promptly acted upon;
- identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/pastoral leads;
- whenever overseeing the use of technology (devices, the Internet, new technology, etc.) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (check what appropriate filtering and monitoring processes are in place);
- carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law;
- prepare and check all online sources and resources before using in the classroom;
- encourage pupils to follow their Acceptable Use Agreement, regularly remind them about it and enforce school sanctions where there is a breach of the Agreement;
- notify the DSL of new trends and issues before they become a problem;
- take a zero-tolerance approach to bullying and low-level sexual harassment either offline or online;
- receive and act upon regular updates from the DSL and have a professional curiosity for online safety issues;
- model safe, responsible, and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and the professional reputation of all staff;
- ensure that any digital communications with pupils are on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones or social media messaging or posts.

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).
- ensure the security of their username and password for the school system, not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- understand the importance of reporting abuse, misuse or access to inappropriate materials including those involving hoaxes and on-line challenges and know how to do so;
- know what action to take if they or someone they know feels worried or vulnerable when using online technology;
- understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use agreements cover their actions out of school, including on social media;
- know and understand school procedures on the use of mobile phones and other digital devices;

- know and understand school procedures on cyberbullying/sharing nude and/or semi-nude images and/or videos;
- understand that the school has imposed filtering rules and will monitor the use of school owned digital devices for inappropriate access to, or downloads from, websites. Breaches may lead to sanctions as described in the Behaviour policy and, in some cases, may involve the Police;
- understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school if there are problems.

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;
- work with and support the school when issues or concerns are identified which are as a result of the school's filtering and monitoring procedures and processes.

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.

- plan 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 need to give consent to when they log into the school network at least annually;
- ensures staff will model safe and responsible behaviour in their own use of technology during lessons;
- 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 its 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 required 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

7.1 School Community and Parental Responsibilities:

- 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;
- 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;
- 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;

7.2 Pupil Responsibilities:

- Pupils are not allowed on social networking sites at school;
- 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;
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private;

7.3 Parental Responsibilities:

- 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);

7.4 Staff Responsibilities:

- Staff users must not reveal the names of staff, pupils, parents or any other member of the school community on any social networking site;
- 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;
- Newsgroups will be blocked unless a specific use is approved;
- 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

- We will follow the advice from the National Cyber Security Center and, where possible, we will use password managers, advise on selecting strong passwords, avoid reuse and use multi-factor authentication.
- Passwords or encryption keys must not be recorded on paper or in an unprotected file;
- 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 DEVICES

- 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 not permitted to have mobile phones out during the school day, including break and lunchtimes;
- 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 **must not** 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 DEVICES

- 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 USE OF PRIVATE ONLINE TUTORS IN BOARDING

14.1 Parents of boarding students are expected to undertake the following actions and notify the boarding house staff if they intend to organise private online tuition for their child whilst they are in the Lairthwaite boarding house:

- Make every reasonable effort to check that the tutor is working for a reputable company with their own safeguarding policies;
- If it is an independent tutor parents must endeavour to seek out any testimonials or references that could be verified by them;
- Ask if the tutor has a DBS check (this is not compulsory for independent tutors but it would be the gold standard);
- Check if they are a member of The Tutors' Association (this is not compulsory for tutors but it shows that they want to have some form of registration as a legitimate tutor);
- Ask for contact details such as phone number, email etc;
- Where possible tuition should take place in a relatively public area (not in dorms); older students can have more leeway with this;
- Boarding must be made aware that private tuition has been organised. This must include the details of the tutor and times and dates of tuition;
- Tuition should not be shared by students unless all parents have given permission;
- Any issues that the student tells their parents about which cause concern, must immediately be shared with boarding staff.

15.0 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.

16.0 INCIDENT REPORTING

- Online safety incidents involving a pupil must immediately be reported to the DSL via CPOMS;
- Online safety incidents involving a member of staff must immediately be reported to the Head teacher.

17.0 RESPONDING TO INCIDENTS OF MISUSE

17.1 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.

17.2 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.

17.3 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.

18.0 COMPLAINTS

18.1 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.

18.2 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).

18.3 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.

18.4 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.

18.5 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.

18.6 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

STAFF / VOLUNTEER
ACCEPTABLE USE POLICY AGREEMENT

The use of Information and Communication technologies (IT and personal data) such as email, the Internet, and mobile devices are an expected part of working life in school. This Agreement is designed to ensure that all staff and volunteers are aware of their responsibilities when using any form of IT. It applies to any IT used in school, the use of school-owned devices, and IT systems out of school and the use of personal equipment/devices in school or in situations related to their employment by the school. All staff and volunteers (where they are using technology in school or in connection with the work of school) are expected to sign this Agreement and always adhere to its content. Any concerns or clarification should be discussed with **Wendy Lightfoot** (Online Safety Lead) or **Simon Jackson** (Head teacher).

This Acceptable Use Agreement is intended to ensure that:

- staff and volunteers are responsible users and stay safe while using technologies for educational, personal, and recreational use;
- school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff are protected from potential risk from the use of IT in their everyday work and work to ensure that the children or young people in their care are safe users.

Acceptable Use Policy 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.

Keeping Safe

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will only use my own usernames and passwords which I will choose carefully so they cannot be guessed easily and must be complex (multi-factor authentication will be used where possible).
- I will not use any other person's username and password.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media sites, to pupils.
- I will ensure that my data is regularly backed up.
- I will ensure that I 'log off' after my network session has finished.
- I will always lock my computer if I have to leave the room.
- If I find an unattended machine logged on under another user's username, I will **not** continue using the machine – I will 'log off' or lock it immediately.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will not accept invitations from school pupils to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.
- As damage to professional reputations can inadvertently be caused by quite innocent postings, text or images, I will also be careful with who has access to my pages, especially with other parents and their children.
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when it is deemed necessary that I am required by law or by school procedures to disclose it an appropriate authority.
- I will only transport, hold, disclose or share personal information as per the data protection policy.
- Where personal data is transferred outside the secure school network, it must be encrypted. Personal data can only be taken out of school or accessed remotely when authorised, in advance, by the Head teacher or Governing Body. Personal or sensitive data taken off site in an electronic format must be encrypted, e.g. on a password secured laptop or memory stick. Staff leading a trip are expected to take relevant pupil information with them but this must be held securely at all times.
- I will ensure that any private social networking sites/blogs etc. that I create, or actively contribute to:
  - do not reveal confidential information about the way the school operates;
  - are not confused with my school responsibilities in any way;
  - do not include inappropriate or defamatory comments about individuals connected with the school community;
  - support the school's approach to online safety which includes not uploading or posting to the internet any pictures, video or text that could upset, offend or threaten the safety of any member of the school community or bring the school into disrepute;
- I will not attempt to bypass the school network filtering (Sophos), monitoring (Impero) and security systems (Sophos) in place.
- I will only use my personal IT in school for permissible activities and I will follow the rules set out in this agreement. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

Promoting Safe Use by Learners

- I will support and promote the school's Online Safety, Data Protection and Behaviour Policies and help pupils to be safe and responsible in their use of IT and related technologies.
- I will model safe use of the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school procedures if an issue arises in school that might compromise a learner, user or school safety or if a pupil reports any concerns.

Communication

- I will only use the school's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed 'acceptable' by the Head teacher or Governing Body.
- I will communicate on-line in a professional manner and tone, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. Anonymous messages are not permitted.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- I will only communicate with pupils and parents using the school's approved, secure email system(s). Any such communication will be professional in tone and manner.
- I am aware that any communication could be forwarded to an employer or governors or in some circumstances, the police.
- I will only use chat and social networking sites that are approved by the school when using school-owned devices or the school IT network.
- I will not use personal email addresses on the school IT systems unless I have permission to do so.

Research and Recreation

- I will not browse, upload, download, distribute or otherwise access any materials which are illegal, discriminatory or inappropriate or may cause harm or distress to others.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity.
- I know that all school IT is primarily intended for educational use and I will only use the systems for personal or recreational use if this is allowed by the school.

Sharing

- I will not access, copy, remove or otherwise alter any other user's file, without their permission.
- I will always respect the privacy and ownership of others' work online at all times and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission, and will credit them if I use it.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos). If I am unsure about this, I will seek advice.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes using school equipment in line with school procedures.
- I will only take images/video of pupils and staff where it relates to agreed learning and teaching activities and will ensure I have parent/staff/others' permission before I take them.
- If images are to be published on-line or in the media I will ensure that parental/staff permission allows this.

- I will not use my personal equipment to record images/video unless I have permission to do so from the Head teacher or other Senior Manager.
- I will not keep images and/or videos of pupils stored on my personal equipment unless I have permission to do so. If this is the case, I will ensure that these images cannot be accessed or copied by anyone else or used for any purpose other than that for which I have permission.
- Where these images are published (e.g. on the school website/prospectus), I will ensure that it is not possible to identify the people who are featured by name or other personal information.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

Buying/Selling/Gaming

- I will not use school equipment for personal on-line purchasing, selling or gaming unless I have permission to do so.

Problems

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the DSL or Head teacher.
- I will not install any hardware of software on a computer or other device without permission of the IT Network Manager.
- I will not try to alter computer settings without the permission of the IT Network Manager.
- I will not cause damage to IT equipment in school.
- 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 the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that if I fail to comply with this agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I will use the school network in a responsible way and observe all the restrictions as explained in this agreement. I agree to use IT by these rules when:

- ✓ I have permission to use school IT systems and school-owned devices at school, at home, or in other public or private spaces.
- ✓ I use my own IT (where permitted) in school and will adhere to the school staff Code of Conduct in relation to the use of my own personal devices/technology.
- ✓ I use my own IT out of school to access school sites or for activities relating to my work or volunteering for school.

Appendix 2

Acceptable IT Use - Students

The use of IT (including the use of the internet, Google Apps for Education, email and other online resources) is an important part of learning. We expect everyone to be safe and responsible when using IT. It is essential that students are aware of online safety and their responsibilities under the terms of this agreement.

For my own personal safety:

- I understand that the school IT network (internet, email, digital video etc.) is intended for educational use.
- I understand my use of the school IT network (internet, email, digital video etc.) will be monitored.
- I understand that any data that is captured as part of using the school IT network is stored and accessed in compliance with the school's Data Protection Policy (KSMAT/STAT/023).
- I will only log onto the school IT network with my own username and password and I will not share them.
- I will 'log off' when leaving a computer.
- I will report 'inappropriate contacts' when I am communicating online.
- I will not disclose or share personal information about myself or others online.
- I will not search for, access, upload or download any material that purveys a radical or extremist view.
- 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 act towards others as I expect others to act towards me:

- I will respect others' work and will not access, copy, remove or otherwise alter any other user's files without their knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions to my own.
- I will only take images/recordings of others if I have permission to do so by my teacher for school purposes.
- I will not use my personal device e.g. smart watch to capture images, video or voice recordings whilst on the school premises.
- I will not distribute images/recordings of others without their permission.

I understand that everyone has an equal right to use IT as a resource:

- I will not use the school IT network for personal use unless I have permission to do so.
- I will not make large downloads/uploads that might take up internet capacity and prevent others from being able to carry out their work, unless I have permission to do so.
- I will not use the school IT network for online gaming, online gambling, internet shopping, file sharing or video broadcasting (e.g. YouTube) unless I have permission to do so.

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

- I will only use my personal hand-held (ipad/smart watch and/or external devices (USB devices) 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.
- I will not upload, download or access any material that could be considered offensive, 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 not sign up for any online service unless this is approved by my teacher.
- I will immediately report any damage/faults to IT equipment or software, however this may have happened.
- I will not open any email attachments, unless I know and trust the person or organisation it comes from, to minimise the risk of downloading a virus or another harmful programme.
- I will not install or attempt to install or store programmes of any type on a school computer, nor will I try to alter school computer settings.
- I will only save files to the school IT network and Google Drive that are related to my school work.
- I will check my email regularly and carry out routine "housekeeping" by deleting any unnecessary messages.

When using the internet for research or educational purposes:

- I will ensure that I have the permission to use the original work of others in my own work, or acknowledge other people's work or website addresses where I cannot obtain such permission.
- I will not try to download copies and use work that is protected by copyright law (including music and videos).
- I will take care to check that the information I access on the internet 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 any work produced using artificial intelligence (AI) must be acknowledged in my work and that I should seek advice from my teacher about whether this is acceptable or not.
- In terms of non-examined assessments for qualifications, I understand that AI misuse could result in malpractice and that I must work in accordance to the Joint Council for Qualifications (JCQ) rules.

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

- I will ensure that my online activity (including uploading images, video, sounds or texts) will not cause others distress, anxiety or bring the school into disrepute. This includes anything that concerns my membership of the school community (e.g. cyberbullying, use of personal information/images etc.)
- **I understand that all my use of the Internet via school-owned devices and the IT network and other related technologies will be monitored and logged and can be made available to my teachers, parent/guardian and/or the police.**
- **I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied (this may include loss of access to the school's IT network/internet, detention or exclusion) and my parent/guardian will be contacted, and any illegal activities will be reported to the police.**

Declaration

We have read, understood and agree to follow the terms and conditions outlined in this agreement when:

- I use the school-owned IT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. smart technology, camera, USB stick, etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, Google Classroom or other online resources, websites etc.

Keswick School will not be able to give students access to the school IT system if consent is not given to this agreement.

Please confirm that you have read, understood and accept all of the expectations and rules set out in this agreement.

Appendix 3

Acceptable IT Use – Parent/Guardian

The use of IT (including the use of the internet, Google Apps for Education, email and other online resources) is an important part of learning. We expect everyone to be safe and responsible when using IT. It is essential that students are aware of online safety and their responsibilities under the terms of this agreement.

Parents/guardians are asked to read and then give their consent to the following agreement.

For my own personal safety:

- I understand that the school IT network (internet, email, digital video etc.) is intended for educational use.
- I understand my use of the school IT network (internet, email, digital video etc.) will be monitored.
- I understand that any data that is captured as part of using the school IT network is stored and accessed in compliance with the school's Data Protection Policy (KSMAT/STAT/023).
- I will only log onto the school IT network with my own username and password and I will not share them.
- I will 'log off' when leaving a computer.
- I will report 'inappropriate contacts' when I am communicating online.
- I will not disclose or share personal information about myself or others online.
- I will not search for, access, upload or download any material that purveys a radical or extremist view.
- 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 act towards others as I expect others to act towards me:

- I will respect others' work and will not access, copy, remove or otherwise alter any other user's files without their knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions to my own.
- I will only take images/recordings of others if I have permission to do so by my teacher for school purposes.
- I will not use my personal device e.g. smart watch to capture images, video or voice recordings whilst on the school premises.
- I will not distribute images/recordings of others without their permission.

I understand that everyone has an equal right to use IT as a resource:

- I will not use the school IT network for personal use unless I have permission to do so.
- I will not make large downloads/uploads that might take up internet capacity and prevent others from being able to carry out their work, unless I have permission to do so.
- I will not use the school IT network for online gaming, online gambling, internet shopping, file sharing or video broadcasting (e.g. YouTube) unless I have permission to do so.

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

- I will only use my personal hand-held (ipad/smart watch and/or external devices (USB devices) 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.
- I will not upload, download or access any material that could be considered offensive, 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 not sign up for any online service unless this is approved by my teacher.

- I will immediately report any damage/faults to IT equipment or software, however this may have happened.
- I will not open any email attachments, unless I know and trust the person or organisation it comes from, to minimise the risk of downloading a virus or another harmful programme.
- I will not install or attempt to install or store programmes of any type on a school computer, nor will I try to alter school computer settings.
- I will only save files to the school IT network and Google Drive that are related to my school work.
- I will check my email regularly and carry out routine "housekeeping" by deleting any unnecessary messages.

When using the internet for research or educational purposes:

- I will ensure that I have the permission to use the original work of others in my own work, or acknowledge other people's work or website addresses where I cannot obtain such permission.
- I will not try to download copies and use work that is protected by copyright law (including music and videos).
- I will take care to check that the information I access on the internet 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 any work produced using artificial intelligence (AI) must be acknowledged in my work and that I should seek advice from my teacher about whether this is acceptable or not.
- In terms of non-examined assessments for qualifications, I understand that AI misuse could result in malpractice and that I must work in accordance to the Joint Council for Qualifications (JCQ) rules.

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

- I will ensure that my online activity (including uploading images, video, sounds or texts) will not cause others distress, anxiety or bring the school into disrepute. This includes anything that concerns my membership of the school community (e.g. cyberbullying, use of personal information/images etc.)
- **I understand that all my use of the Internet via school-owned devices and the IT network and other related technologies will be monitored and logged and can be made available to my teachers, parent/guardian and/or the police.**
- **I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied (this may include loss of access to the school's IT network/internet, detention or exclusion) and my parent/guardian will be contacted, and any illegal activities will be reported to the police.**

Declaration

We have read, understood and agree to follow the terms and conditions outlined in this agreement when:

- I use the school-owned IT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. smart technology, camera, USB stick, etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, Google Classroom or other online resources, websites etc.
-

Keswick School will not be able to give students access to the school IT system if consent is not given to this agreement.

Edulink, that you (parent/guardian) have read, understood and accept all of the expectations and rules set out in this agreement. We also request that parents/guardians take care to ensure that appropriate systems are in place at home to protect and support your children online.

Appendix 4

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 5

Acceptable Use of IT – Governors, Volunteers and Visitors

Acceptable use of the school's ICT facilities and the internet: agreement for Governors, Volunteers and Visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6

FILTERING AND MONITORING ARRANGEMENTS

1.0 INTRODUCTION

1.1 The Department for Education's (DfE) statutory guidance 'Keeping Children Safe in Education' obliges schools in England to "ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to risks from the school's IT system" however, we will "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

1.2 To further support schools to meet digital and technology standards, the DfE have published Filtering and Monitoring Standards. In addition to aspects of both filtering and monitoring systems, these standards detail the allocation of roles and responsibilities, and that schools should be checking their filtering and monitoring provision at least annually. Given the extent of personal data involved with some monitoring solutions, we will consider undertaking a data protection impact assessment.

1.3 'Keeping Children Safe in Education' also requires that **all** staff should receive, at induction, appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring). The training will be regularly updated. In addition, all staff receive safeguarding and child protection (including online safety) updates (for example, via email and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

1.4 It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety, including arrangements for filtering and monitoring, empowers the school to protect and educate pupils, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

1.5 The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel our pupils, students or staff are at risk, we will report incidents to the Anti-Phishing Working Group (https://apwg.org/).

1.6 Filtering and monitoring systems are used to keep pupils safe when using the school's IT system. Filtering systems block access to harmful sites and content. Monitoring systems identify when a user accesses or searches for certain types of harmful content on school devices (it doesn't stop someone

accessing it). The school is then alerted to any concerning content so that appropriate interventions and ultimate responses can be made.

1.7 All staff and others who can access school devices will be provided with a copy of the school Code of Conduct on induction which sets out information in relation to the acceptable behaviour standards, including those for use of school devices (either in school or off-site). All staff, pupils (or parents/carers on the child's behalf) and Governors will be required to read and sign the Online Acceptable Use agreement on induction for the use of school devices (either in school or off-site).

Required Outcome	**Responsibility**	**Named responsible individual(s)**
Identify and assign a member of the Senior Leadership Team (SLT) to be responsible for ensuring that the standards are met.	Governors	Simon Jackson/ Emily Wilson
Identify and assign a Governor to be responsible for ensuring that the standards are met.	Governors	Emily Wilson
Identify and assign the roles and responsibilities of staff (e.g. school online safety coordinator, Designated Safeguarding Lead) and third parties (e.g. external service providers).	Governors	Personnel Committee + Finance Committee
Document decisions about what is blocked or allowed and why.	SLT	Wendy Lightfoot / Steven Waning
Review the effectiveness of our provision (and provide evidence e.g. communication between technical staff and Designated Safeguarding Leads (DSLs).	SLT	Wendy Lightfoot
Oversee reports.	SLT	Wendy Lightfoot / Steven Waning
Ensuring all staff have received appropriate and up to date training, follow Policies, procedures and processes around online safety and filtering and monitoring.	SLT	Simon Jackson / Wendy Lightfoot
Ensuring all staff act on reports and concerns.	SLT	Wendy Lightfoot
Oversee and act on filtering and monitoring reports.	DSL	Steven Waning
Oversee and act on safeguarding concerns.	DSL	Wendy Lightfoot
Oversee and act on checks to monitoring systems.	DSL	Steven Waning
Maintain filtering and monitoring systems.	IT service provider	Steven Waning Sophos / Impero
Provide filtering and monitoring reports.	IT service provider	Sophos / Impero
Complete actions following concerns or checks to systems.	IT service provider	Steven Waning Sophos / Impero

Carry out reviews of the filtering and monitoring provision at least annually.	DSL/Head/DPO/IT Network Manager Sophos/Impero
Carry out checks which are informed by the review to ensure systems are working as intended.	DSL/Head/DPO/IT Network Manager Sophos/Impero

2.0 DfE FILTERING AND MONITORING STANDARDS

2.1 The DfE published updated guidance in March 2023 which sets out standards that schools should meet in relation to filtering and monitoring. The school will comply with the requirements set out in DfE guidance relating to 'filtering and monitoring standards for schools and colleges', which are summarised below:

2.2 In order to meet these requirements, we will ensure that the following arrangements are in place. We will identify and assign roles and responsibilities to manage our filtering and monitoring systems as follows and outlined above:

- A member of SLT and a Governor will be responsible for ensuring the standards are met.
- The roles and responsibilities of individual staff members and third parties (e.g. external service providers such as IT providers) will be clearly identified.
- The school's IT strategy will be designed by educators to suit the age and curriculum requirements of the pupils. Decisions regarding what content is blocked, and why, will be documented.
- All staff will be given awareness training at induction outlining how our filtering and monitoring systems work. This training will also be included in the annual safeguarding training.

2.3 Day to day management of filtering and monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective. The Head teacher/DSL works closely together with the DPO/IT Network Manager and IT service providers to meet the needs of our setting.

2.4 The DSL/IT Network Manager take responsibility for safeguarding and online safety, in the following areas:

- filtering and monitoring reports;
- safeguarding concerns;
- checks to filtering and monitoring systems.

2.5 The IT service provider has technical responsibility for:

- maintaining filtering and monitoring systems;
- providing filtering and monitoring reports;
- completing actions following concerns or checks to systems.

2.6 The IT Network Manager / IT service provider work to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

3.0 BLOCKING HARMFUL AND INAPPROPRIATE CONTENT

3.1 No filtering system can be 100% effective and we understand the coverage of our filtering system, any limitations it has, and take mitigating measures accordingly to minimise harm and to meet our statutory duties outlined in Keeping Children Safe in Education and the Home Office Prevent Duty.

3.2 We will ensure that our filtering system blocks harmful and inappropriate content, including all sites on the Internet Watch Foundation (IWF) list, without unreasonably impacting teaching and learning or restricting students from learning how to assess and manage risk themselves. As a minimum we will ensure that our filtering system manages the following content (and web search)

Content	**Explanatory notes – content that:**
Discrimination	Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010.
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances.
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance.
Gambling	Enables gambling.
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content.
Pornography	Displays sexual acts or explicit images.
Piracy and copyright theft	Includes illegal provision of copyrighted material.
Self-Harm	Promotes or displays deliberate self-harm (including suicide and eating disorders).
Violence	Displays or promotes the use of physical force intended to hurt or kill.

3.3 In order to ensure that our filtering system blocks harmful and inappropriate content the following arrangements will apply:

- the Governing Body will support SLT to procure and set up systems which meet this standard;
- we will follow the guidance set out for schools by the UK Safer Internet Centre (UKSIC) on 'Appropriate Filtering for Education Settings' to inform our approach to establishing appropriate levels of filtering;
- we will ensure that our filtering provider is a member of the Internet Watch Foundation; is signed up to the Counter-Terrorism Internet Referral Unit list (CTIRU) and blocks access to illegal content including child sexual abuse material (CSAM);
- we will ensure that our filtering system is operational, up to date and applied to all users (including guest user accounts); school owned devices and devices using the school broadband connection;
- our filtering provider will be asked for system specific training and support for the DSL and IT staff as required;
- we will regularly check that our filtering system remains current by using the internet filter test tool created and hosted by South West Grid for Learning (swgfl.org.uk)

4.0 FILTERING

4.1 For filtering to be effective, it should meet the needs of both pupils and staff and reflect specific use of technology whilst minimising potential harms. An active and well managed filtering system is an important part of providing a safe environment for pupils to learn.

4.2 Our filtering system:

- filters all internet feeds, including any backup connections;
- is age and ability appropriate for the users, and is suitable for our setting;
- handles multilingual web content, images, common misspellings and abbreviations;
- identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and blocks them;
- provides alerts when any web content has been blocked;

4.3 It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as a member of SLT and/or the DSL.

4.4 Our filtering systems allow us to identify the:

- device name or ID, IP address, and where possible, the individual
- time and date of attempted access
- search term or content being blocked

4.5 The school has a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be made aware of this procedure. If staff or pupils discover unsuitable sites, the URL will be reported to the DSL who will then record the incident and escalate the concern as appropriate. Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, the Police or CEOP.

5.0 MONITORING

5.1 We will employ effective monitoring strategies that meet the safeguarding needs of our school. Whilst we recognise that no monitoring can be 100% effective, we will ensure that, as a minimum, our monitoring system covers the following content:

Content	**Explanatory notes – content or communications that:**
Illegal	Is illegal (e.g. Child abuse images and terrorist content). It is important that safeguards for illegal content cannot be disabled by the user.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.
Discrimination	Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010.
Drugs/Substance abuse	Displays or promotes the illegal use of drugs or substances.

Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance.
Gambling	Enables gambling.
Pornography	Displays sexual acts or explicit images.
Self-Harm	Promotes or displays deliberate self-harm (including suicide and eating disorders).
Violence	Displays or promotes the use of physical force intended to hurt or kill.
Suicide	Suggest the user is considering suicide.

5.2 In order to achieve this, the following arrangements will apply.

- We will follow the guidance set out for schools by the UK Safer Internet Centre on 'Appropriate Monitoring for Schools' to inform our monitoring strategy.
- The Governing Body will support the SLT to make sure effective device monitoring is in place which meets this standard and the risk profile of the school.
- the DSL will take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.
- Training will be provided to ensure that the specialist knowledge of both safeguarding and IT staff remains current.
- Staff will provide effective supervision, take steps to maintain awareness of how devices are being used by pupils/others and report any safeguarding concerns to the Head teacher/DSL.

5.3 Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not prevent users from accessing material through internet searches or software.

5.4 Monitoring allows the school to review user activity on our devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing us to take prompt action and record the outcome.

5.5 Our monitoring strategy is informed by the filtering and monitoring review. A variety of monitoring strategies are required to minimise safeguarding risks on internet connected devices and include:

- physically monitoring by staff watching screens of users;
- live supervision by staff on a console with device management software;
- network monitoring using log files of internet traffic and web access;
- individual device monitoring through software or third-party services.

5.6 The Governing Body/Board of Trustees support SLT to review the effectiveness of our monitoring strategies and reporting process. We will always make sure that incidents are urgently picked up, acted on and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. It is clear to all staff how to deal with these incidents and who should lead on any actions.

5.7 Device monitoring is managed by the IT Network Manager / Impero. They will:

- ensure monitoring systems are working as expected;
- provide reporting on pupil device activity at intervals to be determined by the school;
- receive safeguarding training including online safety;
- record and report safeguarding concerns to the DSL;

5.8 Those involved will also ensure that:

- monitoring data is received in a format that staff can understand;
- users are identifiable to the school, so concerns can be traced back to an individual, including guest accounts.

6.0 REVIEW OF FILTERING AND MONITORING

6.1 The Governing body/Trustees have overall strategic responsibility for meeting the standard which relates to the review of filtering and monitoring. They should make sure that filtering and monitoring provision is reviewed at least annually and may form part of a wider online safety review.

6.2 Reviews of filtering and monitoring are carried out to identify our current provision, any gaps, and the specific needs of any pupils and staff.

6.3 Prior to undertaking the review, we will consider the following:

- the risk profile of our pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL);
- what our filtering system currently blocks or allows and why;
- any outside safeguarding influences, such as county lines;
- any relevant safeguarding reports;
- the digital resilience of our pupils;
- teaching requirements, for example, our RHSE and PSHE curriculum;
- the specific use of our chosen technologies, including Bring Your Own Device (BYOD);
- the related safeguarding or technology policies we already have in place;
- the checks that are currently taking place and how resulting actions are handled.

6.4 As a result, and to ensure it remains effective, our review of filtering and monitoring will inform:

- related safeguarding or technology policies and procedures;
- roles and responsibilities;
- any gaps in training for staff;
- curriculum and learning opportunities;
- procurement decisions;
- how often and what is checked;
- monitoring strategies.

6.5 Although the DfE standards recommended that the review of the filtering and monitoring systems is undertaken at least annually, we will also consider a review when:

- a safeguarding risk is identified;
- there is a change in working practice, like remote access or BOYD;
- new technology is introduced.

6.6 As part of the review process, there are a number of external tools which can be used to support the school:

- SWGfL 360 degree safe toolkit
- LGFL Online Safety Audit
- UKCIS (UK Centre for Internet Safety) 'Questions from the governing board'

- UKCIS Online Safety Audit Tool for trainee and early career teachers
- UKCIS 'External visitors guidance'

6.7 The review is conducted by the Head teacher/DSL/DPO/IT Network Manager and the IT service provider and, where necessary the responsible governor will be involved. The results of the online safety review will be recorded on the SWGFL Filtering and Monitoring Checklist Register (or similar), actioned and shared with staff as appropriate and made available to those entitled to inspect that information.

6.8 Reviews may be conducted more frequently if a safeguarding risk is identified or there is a change in working practice (e.g. remote access or BOYD) or if new technology is introduced. Changes to the school filtering procedures will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from SLT. The outcomes from all filtering and monitoring reviews will be recorded.

6.9 We will undertake checks of our filtering provision, the regularity of which will be based on the context, the risks highlighted in the filtering and monitoring review and any other risk assessments. Any checks will be undertaken from both a safeguarding and IT perspective. We can also make use of the South West Grid for Learning filtering testing tool which checks that our filtering system is blocking access to illegal child sexual abuse material; unlawful terrorist content; and adult content.

6.10 When checking our filtering and monitoring systems, we will ensure that the system setup has not changed or been deactivated and the checks will include a range of:
- school owned devices and services (for both pupils and staff), including those used off site;
- implications in relation to geographical areas across the school site;
- user groups, e.g. teachers, pupils and guests.

6.11 Records will be held in the form of a System filtering and monitoring checks record/log so that they can be reviewed. Our record/log will include:
- when the checks took place;
- who did the check;
- what they tested or checked;
- resulting actions.

6.12 Checks might include any or all of the following:
- settings and updates on, for example, Google for Education;
- all in-school staff device password and log-on checks, including those which are used in the home environment;
- pupil and staff account compliance checks;
- maintenance of subscriptions and licences;
- revision and review of policies and procedures.

7.0 REPORTING SAFEGUARDING AND TECHNICAL CONCERNS

7.1 All staff are aware of the reporting mechanisms in place for reporting concerns about safeguarding and technical issues. Staff are advised to report if:
- they witness or suspect unsuitable material has been accessed;
- they can access unsuitable material;

- they are teaching topics which could create unusual activity on the filtering logs ;
- there is failure in the software or abuse of the system;
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks;
- they notice abbreviations or misspellings that allow access to restricted material.

8.0 FILTERING AND MONITORING RESOURCE LISTS

DfE Keeping children Safe in Education
DfE Broadband internet standards for schools and colleges
DfE Filtering & monitoring standards for schools and colleges
DfE Cyber security standards for schools and colleges
LGfL Free Training on Filtering and Monitoring
LGfL Online Safety Audit Toolkit
Smoothwall Benchmarking Your Digital Safeguarding - Strategies for Ofsted
SWGfL Filtering and Monitoring Checklist Register
SWGfL 360o Safe - Online safety review tool
UKSIC Guidance on Appropriate Filtering
UKSIC Guidance on Appropriate Monitoring
UKSIC Online safety in schools and colleges: Questions from the Governing Board 2022
UKSIC Webinar: Introduction to Filtering & Monitoring
UKSIC Webinar: Overview of Filtering & Monitoring Standards
UKSIC Webinar: Filtering & Monitoring Systems - Assessing Risk
UKSIC Webinar: Filtering & Monitoring Safeguards
UKSIC Webinar: Filtering & Monitoring Responsibilities & Documenting

9.0 ONLINE SAFETY LINKS

9.1 This list provides links to relevant government guidance and a range of national organisations who can offer support to schools.

9.2 Related guidance is available on:
- relationships and sex education (RSE) and health education
- national curriculum in England computing programmes of study
- national curriculum in England citizenship programmes of study

9.3 Support and resources are also available from:
- National Centre for Computing Education (NCCE)
- UK Council for Internet Safety
- UK Safer Internet Centre (UKSIC)
- Education for a Connected World
- CEOP (Child Exploitation and Online Protection Centre)
- CEOP Education Programme (Thinkuknow.co.uk)
- Cumbria Safeguarding Children Partnership (Cumbria SCP)
- Information Commissioner's Office (ICO)
- Teaching online safety in schools
- The PREVENT Duty – DfE non-statutory Departmental advice for Schools and Childcare Providers

- How social media is used to encourage travel to Syria and Iraq: briefing note for schools – Home Office advice
- Internet Watch Foundation (IWF)
- Smoothwall

9.4 Schools can also get advice from national organisations such as:

- Anti-Bullying Alliance
- Association for Citizenship Teaching
- The Diana Award
- DotCom Charity
- Hopes and Streams
- Internet Matters
- NSPCC learning
- Parent Zone's school resources
- PSHE Association
- SWGfL
- Better Internet for Kids
- Virtual Global Taskforce — Report Abuse
- Cyberbullying.org

9.5 You can refer parents to the following national organisations for support:

- Internet Matters
- NSPCC
- Parent Zone
- Facebook Advice to Parents
- Family Online Safety Institute (FOSI)
- Get safe online - Test your online safety skills

9.6 You can refer pupils to the following national organisations for support:

- BBC Own It
- Childline
- Childnet