Kesgrave High School

Online Safety Policy

This policy reviewed **annually, in conjunction with the Safeguarding Policy**

Policy Approval

Where	**Chair**	**When**
Enabling Excellence	David Bevan	23 November 2022

Chair of Governors	Sue White
Headteacher	Julia Upton

Policy History

Issue No.	Author	Date written	Approved by governors	Comments
1	J Logan	3 Oct 2020		
2	T Rush	6 Oct 2020		Ammendments made by T Rush
3	T Rush	20 Nov 2021	24 Nov 2021	In line with KCSiE and Safeguarding Policy
4	T Rush	14.11.22	23.11.22	

Contents

Online Safety Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. 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 only be taken over issues covered by the published Behaviour Policy.

Online safety is viewed as part of a schools statutory safeguarding responsibility.

The school will deal with such incidents within this policy and associated issues that will incorporate the behaviour, safeguarding, mobile phone and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviours that take place out of school.

KCSIE 2022 references four areas of risk online within part two: content, contact, conduct and commerce.

1 Roles and Responsibilities

The online safety roles and responsibilities of individuals and groups within the school are defined below.

1.1 Headteacher

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Leads (see Appendix A).

The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff.

The Senior Leadership Team will receive regular monitoring reports from the Online Safety Leads and incidents are logged on the school system and in safeguarding files where appropriate.

The Headteacher will include a summary of any Online Safety matters within his report to the Governors.

1.2 Online Safety Team (Appendix A)

The Online Safety Team:

- takes day-to-day responsibility for online issues and has a leading role in establishing and reviewing the schools online safety policies / documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- provides training and advice for staff, students, parents / carers and the wider community of the school;
- liaises with the Trust, the Local Authority and other relevant bodies;
- liaises with school technical staff;
- receives reports of online incidents and creates a log of incidents to inform future online developments;
- meets regularly with the Online Safety Governor to discuss current issues;
- attends relevant meeting / committee of Governors and will report specifically to the Enabling Excellence Committee, and
- reports regularly to Senior Leadership Team.

1.3 Network Manager

The Network Manager (with support from the wider technical staff) is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- that users may only access the networks and devices that they are authorised to;
- that they keep up-to-date with online technical information in order to effectively carry out their online role and to inform and update others as relevant;
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Senior Leadership Team and Online Safety Leads as appropriate for investigation / action / sanction, and
- that monitoring software / systems are implemented and maintained up to date.

1.4 Teaching and Support Staff

The Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices;
- they report any suspected misuse or problem to the Headteacher or Online Safety Leads for investigation / action / sanction;
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems;
- online issues are embedded in all aspects of the curriculum and other activities;
- students understand and follow the Online Safety Policy and Mobile Phone expectations;
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches, and
- Virtual lessons are delivered in line with the 'Virtual Lessons with Students' Guidance (Appendix B).
- They follow the online guidance as detailed in the KHS staff handbook

1.5 Child Protection / Safeguarding Designated Person / Officer

The safeguarding team understand that the risks we educate our students on ‘off line’ will often expose them to greater risks ‘online’ with regard to current safeguarding issues

- The safeguarding team should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:sharing of personal data;
- access to illegal / inappropriate materials including taking, passing and receiving inappropriate images via devices or social media accounts; in line with current guidance (UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people guidance)
- inappropriate on-line contact with adults / strangers / child on child;
- potential or actual incidents of grooming;
- cyber-bullying, and
- uploading of inappropriate material.

1.6 Students

All students:

- are responsible for using the school digital technology systems in accordance with the Student’s Click Clever, Click Safe – Online Safety Acceptance Form (Appendix C);
- are taught to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so; including cyberbullying/child on child abuse
- will be expected to know and understand the rules / expectations on the use of mobile devices and digital cameras. They should also know and understand law in relation to the taking / distributing and receiving inappropriate material / images and the law / school sanctions in relation to Cyber-Bullying (Malicious Communications Act);
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school’s online safety policy covers their actions out of school, if related to their membership of the school, and
- will ensure virtual lessons are attended and behaviour is in line with the Virtual Lessons – Students Guidance (Appendix B).

1.7 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to assist parents / carers in understanding these issues through parents’ evenings, newsletters, letters, website, training events and information about national / local online safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to reinforce the importance on the appropriate use of technology in line with the online safety policy and mobile phone school expectations ‘On Site Off Site’

2 Education

2.1 Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- a planned online safety curriculum should be provided as part of Computing / PHSEE / other lessons and should be regularly revisited;
- key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities;
- students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information;
- students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- students should be helped to understand the need for the student Click Clever, Click Safe – Online Safety Acceptance Form (Appendix C) and encouraged to adopt safe and responsible use both within and outside school;
- staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches, and
- where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

2.2 Parents / Carers

Some parents and carers may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents/carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities;
- Letters, newsletters, magazines, school website - Parent Zone (located on schools website);
- Parents / Carers evenings / awareness sessions;
- High profile events / campaigns e.g. Safer Internet Day, and
- Reference to the relevant web sites / publications / reporting tools.

2.3 Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the schools Online Safety Policy / Safeguarding and Mobile Phone expectations ;
- the online safety leads will receive regular updates through attendance at external training events and updates vial emails / research;
- this online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days;
- the online safety leads will provide advice / guidance / training to individuals as required, and
- in the event of virtual lessons taking place staff will be supported and offered training and CPD.

2.4 Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety / child protection. This may be offered in a number of ways and may include:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation, and
- Participation in school training / information sessions for governors, staff or parents / carers.

3 Technical – Infrastructure / Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities. Specifically:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements;
- There will be regular reviews and audits of the safety and security of school technical systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to school technical systems and devices;
- All users will be provided with a username and secure password - this is a privilege that can be removed if misused;
- The “ administrator” passwords for the school ICT system, used by the Network Manager are available to the Deputy Headteacher, Assistant Headteachers and Data Manager and are stored in the school safe;
- Internet access is filtered for all users. Illegal content (child sexual abuse images) are filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list. The school provider for Broadband is “Talk Straight (http://www.talk-straight.com/). Talk Straight provide the schools Internet Connection, Firewall and Internet Filter. The internet filter is Netsweeper. Netsweeper are a member of the “Internet Watch Foundation” https://www.netsweeper.com/ https://www.schoolsbroadband.co.uk/e-safety-filtering https://www.schoolsbroadband.co.uk/e-safety-filtering-and-security This is part of the ‘Everything ICT Framework’ which is DfE approved
- The school has provided enhanced user-level filtering for staff, KS5 and students in years 7-11 allowing tailored access for those groups;
- Further monitoring of student activity is made available to Heads of Year via the use of Impero Education Pro (https://www.imperosoftware.co.uk), and
- Talk Straight provide the school with a managed Firewall. This is currently a Fortinet Solution. The school infrastructure and individual workstations are protected by up-to-date virus software (currently Sophos).

4 Use of Digital Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm. Specifically

- when using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites;
- in accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection of an individual’s identity, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images;
- staff and volunteers 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- students must not take, use, share, publish or distribute images of others without their permission;
- photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images;
- students’ full names will not be used anywhere on a website or blog, particularly in association with photographs;
- written permission from parents or carers will be obtained before photographs of students are published on the school website – as agreed in the data collection forms;
- any third party wishing to use images or videos of our students for their own websites/training materials/resources must first seek permission from the school, and
- students’ work can only be published with the permission of the student and parents or carers.

5 Communications

The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

Any digital communication between staff and students or parents / carers (email, Firefly etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

All students will be provided with personal school email addresses for school use purposes only and all students and parents / carers will be provided with an account to access our virtual learning environment (Firefly)

Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies – guidance in online etiquette is provided (Appendix C)

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

6 Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools / academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues (CEOP reporting button is accessible via the schools website);
- Clear reporting guidance, including responsibilities, procedures and sanctions, and
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to individual students / parents / carers;
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school, and
- Security settings on personal social media profiles are encouraged to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior leadership team / online safety leads to ensure compliance and appropriate usage. An allocated number of staff will hold the passwords and have access to update such sites on behalf of the school community.

7 Incident Management

7.1 Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. This includes any material that is posted onto social media platforms that would bring the school or any of our staff/students reputations into disrepute.

7.2 Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the Online Safety / Safeguarding Team (Appendix A) immediately for appropriate guidance and action to be taken.

7.3 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported;
- conduct the procedure using a designated computer that will not be used by young people and, if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure;
- it is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection);
- record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. (except in the case of images of child sexual abuse – see below), and
- once this has been completed and fully investigated the senior management team will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures;
    - Involvement by Local Authority or national / local organisation (as relevant), and
    - Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of ‘grooming’ behaviour;
- the sending of obscene materials to a child;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material, and
- other criminal conduct, activity or materials.

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

Appendix A – Online Safety Team

Online Safety Leads/Safeguarding Team	Roz Coe Teresa Rush
Network Manager	Paul Webster
PSHEE Co-ordinator	Lynsey Warfield
Online Safety Governor	Sue White

Appendix B – Guidance for Virtual Lessons

Guidance for Teachers

Access & Equipment:

If you are using a PC/Laptop you will need to check if you have an inbuilt camera, speakers, microphone etc. If you do not have these then you can attach a webcam (if you want students to see you – this is not necessary to show/share resources such as PowerPoint presentations) and use headsets that incorporate headphones and microphones. You can use a mobile or tablet which will include all of these.

Meetings and virtual lessons will be set via Microsoft Teams. No other medium should be used.

Teams can be accessed via a web browser or an app. You do not need to download any software but if you are using a device such as a tablet you may find the app easier.

Types of meeting/session:

You should aim to hold a virtual lesson, once every few timetabled lessons.

You do not need to run whole lessons via virtual meeting.

Sessions could be run in a more ‘tutorial’ fashion to:

- Introduce a topic and get students started
- Go through a difficult topic
- Feedback on coursework/piece of work
- Hold a ‘clinic’ for students that are struggling

You do not need to use your camera facilities for the meetings, you may wish to share a presentation or other documents.

Where you are not holding a virtual lesson, you are expected to be available via Teams chat to answer any student questions.

Timetabling sessions:

You do not need to have virtual sessions for each lesson, you should use when and if you think it is an appropriate method of teaching and to give an interactive element to students every so often to sustain motivation and engagement.

All lessons (virtual or posted work) should take place during timetabled lesson time for that subject.

If you are expecting students to prepare for a virtual lesson please make sure that a Firefly task is set in advance so that they know. You will also need to setup the virtual meeting via the Team for that class or via the calendar.

If a student(s) is unable to attend, you may wish to post the recording of the session on Firefly afterwards so they can catch up. If you decide to do this, please inform students before you start recording so that they can decide if they wish to turn off their cameras (only 6th form can turn on their camera).

Protocols for use:

Please make sure you:

- Are dressed appropriately
- Are sitting with no personal effects (such as photos etc.) in the background or you use the Teams background blurring or picture facility
- Have no other people (unless they are KHS staff) in the frame

All sessions should be recorded and saved – see teacher guide (separate document). They can be used to post on Firefly if a student missed the session and it would be useful.

Students will have a set of rules for usage. In your first session you may want to agree/establish a set of your own ground rules (that adhere to the school rules) so that you feel comfortable. You should establish if you wish for students to have their microphone off for some or all of the lesson. You may wish to direct contributions to students to reply in the chat or by speaking.

Students will be expected to join meetings with video and microphone feeds switched off. You can ask students to switch these on during the lesson if you think it would be useful. However students can abstain if they feel uncomfortable doing so. In this case they should be directed to use the chat facility within the meeting to ask/answer any questions.

Before you share your screen in a virtual meeting, you must make sure all files that are not relevant to the lesson are closed. The normal GDPR rules and procedures should be followed.

Sessions should not be 1-to-1.

Any misuse by students should be reported using the procedure below.

Behaviour for Learning: Online Procedure – Three Easy Steps

The following guide indicates the lines of communication for staff should a student's behaviour, whilst online, be unacceptable. The list below shows examples of poor behaviour. The list is not exhaustive.

- Inappropriate language
- Inappropriate discussions/posts
- Bullying directed at another student/s or person
- Inappropriate use of the forum
- Jeopardising the content of the chat/forum (hacking/editing docs/editing tasks etc)
- Other (there may be other incidents not listed above)

<u>STEP 1: Is the issue a Safeguarding issue?</u>

Yes: Refer to the Safeguarding team immediately using the email address: safeguarding@kesgrave.suffolk.sch.uk.

No: Move on to the next question.

STEP 2: Can the teacher manage the issue online with a warning?

Yes: Teacher manages the issue online, warning the student about further conduct. Teacher is mindful of the following:

- Content of the warning and visibility to the rest of the group
  - If the warning is a general warning to all students, please use the Teams chat functionality. Please remember to keep language used objective and factual; do not use specific names; keep the message short.
  - If the warning is directly to a student please DO NOT use the Teams chat functionality. Message the student directly using email. Log the incident on SIMs & ensure that the HOY of year is informed.
- Logging the incident. Does the teacher need to take a 'screen grab'* of the incident?

  *(In the top right-hand corner of your key board there is a button labelled 'Prt Scrn'. This button takes a picture of the screen you are on. Press the button. Open a word doc. Right click your mouse. Press 'paste'. You should now have a copy of the incident to save). You could also use the snipping tool for this process.

No: Teacher refers the issue to HOY. They will then:

- Discuss the situation with the teacher to ascertain the details
- A contact home to the offending student's parent/guardian then needs to be made via phone call, within 48 hours. HOY and Teacher to discuss who makes this call.
- A warning is given, including the stress of future conduct and appropriate behaviour online**. Incident logged on SIMs

  **As a school, we want students' behaviour to be appropriate. Should a student consistently cause issues online, this will then be reviewed by the Pastoral team, with the student access to Team meetings being reviewed.

STEP 3: Has the situation been resolved?

Yes: issue is closed.

No: HOY refers the issue to Leadership. Leadership actions:

1. Reviews behaviour of student & nature of incident
2. Decision is made about student access to Team meetings
3. Contact by HOY/Leadership to parent explaining what is going to happen next.

Guidance for Students

Access & Equipment:

If you are using a PC/Laptop you will need to check if you have inbuilt speakers, microphone etc. If you do not have these then you can attach a webcam and use headsets that incorporate headphones and microphones.

You can use a mobile or tablet which will include all of these.

Microsoft Teams can be accessed via a web browser or an app. You do not need to download any software but if you are using a device such as a tablet you may find the app easier.

Student rules for use:

- I am responsible for my behaviour and actions when using this technology.
- I understand that normal school rules apply in the online learning environment and that any inappropriate behaviour/comments will be reported by my teacher
- I understand that all meetings broadcast through teams will be recorded by the teacher and retained by the school. This includes all audio and text communications.
- I will follow the rules regarding video and microphone usage:
    - Video & microphone switched off at the start of the virtual lesson
    - Switch on video & microphone as directed by the teachers, as long as I feel comfortable doing so
    - If I choose not to switch on my microphone I should ask/answer questions via the meeting chat
- I will not screenshot or in any other way record any online meetings.
- I will not post any meeting or associated resources to any third-party platform or social media environment.
- I understand that any inappropriate comments that I make will be reported by my teacher

Types of Meeting

Meetings will be set up using Teams for some of your lessons in order to support your learning. Not every lesson with have a virtual element. Some may expect completion of a task or have a video recording to watch and instruct learning.

While working from home you will be expected to stick to your timetable for your lessons as much as possible. Teachers may deliver live lessons at the time of your normal lesson. In all of the timetabled lesson times the teacher will be available via the Teams live chat. This means that if you stick to doing the work on your normal timetable you can get help at this time.

Live delivery of lessons might include:

- Introduction of a topic to get you started
- Go through a difficult topic
- Feedback on coursework/piece of work
- Hold a ‘clinic’ for students that are struggling

If you cannot attend a scheduled meeting you should let your teacher know in advance of the start of the lesson (If you do not have the equipment to access the technology you should let your HOY know as soon as possible.)

Appendix C – Click Clever, Click Safe

Student Online Safety Acceptance Form

‘BE KIND OR BE QUIET’

These guidelines will help keep everyone keep safe online and encourage positive behaviour both in and out of the KHS school community.

- I will not access any unauthorised websites whilst at school using the school equipment
- I will keep my personal information and passwords safe
- I will check my privacy settings regularly
- I will only send and post messages / images / material which are polite, appropriate and friendly to others online
- I always tell a trusted person if something online makes me or a friend feel unhappy or worried
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online
- I know the school can see what I am doing online whilst using school equipment
- I know that if I do not follow the rules then there will be a consequence to my actions
- I know the school has a mobile phone policy / online safety policy and I will agree to abide by these
- I agree to engage in all aspects of online safety within my lessons
- I understand that the school can and will follow up issues that happen outside of school online should these be raised as a concern in school
- I know the school has a report button on the website for me to report any concerns I have
- I have read and talked about these rules with my parents/carers

Signed: -- **Date:** --