Brookes UK

E-Safety Policy

This policy was approved for publication on: **January 2022**

This policy was reviewed on: **March 2024**

This policy will be next reviewed on: **March 2026**

Introduction

The e-Safety Policy, [online safety] relates to other policies including PSHE, Behaviour, Preventing & Tackling Bullying, Data Protection, and Child Protection and Safeguarding (including Prevent). It has been written with regard to national and Local Authority Policies and guidelines taking into consideration the recommendations in the Keeping Children Safe in Education Guidelines (KCSIE), 2023.

The e-safety policy provides an effective approach to online safety empowering the school to protect and educate the whole school in the use of technology. The school has both an e-Safety Coordinator (Computing Lead) and resident Houseparent who liaise with the Principal who is the school's Designated Safeguarding Lead.

The breadth of issues classified with in online safety is considerable, but have been categorised into three areas of risk;

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful online interaction with other users; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Teaching and Learning

1. **Why the internet and digital communications are important**
The Internet is an essential element in 21st Century life for education, business, communication and social interaction. The School has a duty to provide pupils with quality internet access as part of their learning experience in school and the boarding house. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils working and living in a day and boarding school.

2. **Internet use will enhance learning**
Pupils use internet access that is designed for use in school. It includes filtering and monitoring appropriate for the age of the pupils and takes into account the broader requirements associated with use by boarders in a boarding environment. Throughout the year, and especially at the beginning of a new year, and for new pupils arriving at any other time in the year, pupils will be given clear objectives for Internet usage.

3. **Pupils will be taught how to evaluate Internet content**
The School will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught how to report unpleasant Internet content to any adult in school, a member of the boarding house staff team when in the boarding house, or a parent or guardian when outside of school, and how to report their concerns to CEOP via online links. They are taught how to recognise and report misuse and understand the sanctions for misuse. They will also be taught how to use the internet safely in school and beyond through the PSHE and computing curriculum, through regular assemblies and via talks and briefings in the boarding house.

Managing Internet Access

1. **Security System**
The School's computing and ICT systems are reviewed regularly. Updating and patching is carried out each term. Additional external IT partners provide support and security management of the school's IT infrastructure.

2. **E-Mail**
The school uses Google's G-Suite for Education. Encrypted email is provided within the framework of the G-Suite set of applications. Currently students from Year 3 onwards are allowed to make use of the G-Suite applications. In the boarding house, boarders will have limited access to unfiltered, unrestricted Internet via 3G and 4G personal portable devices, for example, during their free time. A contract of acceptable usage will be agreed upon (see appendix). The House will have an age appropriate policy of collecting in mobile phones and Internet connective devices at bedtimes and during the school day. Sanctions for misuse will include periods of confiscation commensurate with the magnitude of infringement and past offence history.

3. **Published content and the school website**

Personal information is kept secure within the school's MIS. The school's website content is managed internally. The systems are hosted offsite and form part of the school's 'cloud computing' solutions. The Principal will take overall editorial responsibility and ensure the content is accurate and appropriate.

4. **Publishing images and work of pupils**

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Full names will not be used anywhere on the school web site or other online space, particularly in association with photographs. Appropriate consents are sought from parents or carers before photos or pupils' work is published online.

5. **Social networking and personal publishing**

During the school day pupils are not allowed to use their mobile devices unless it is part of their normal way of working (see BYOD policy). The school will educate pupils in their safe use, particularly boarders who have possible access to personal 3G and 4G devices. Pupils are advised never to give out personal details of any kind which may identify them, their friends, their school or their location.

6. **Managing Filtering and Monitoring**

The School ensures that filtering and monitoring systems are in place to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn. These systems provide a separate network for children's use as well as a filtering and monitoring matched against the trigger list issued by the Internet Watch Federation (IWF). Whilst these systems are reviewed and improved regularly, factors such as the age range of the children, the number of pupils, how often they access the school network, as well as costs will determine an appropriate degree of filtering and monitoring. The School does all that it reasonably can to limit children's exposure to inappropriate content, contact and conduct online, whilst realising that a balance needs to be achieved that does not unreasonably restrict what the children can be taught or have access to online. Pupils and staff are advised on safe Internet usage and it is made clear that school ICT is not private and will be monitored. If staff or pupils come across unsuitable online materials, evidence is preserved and the site is reported to our IT Support Company. Monitoring and filtering forms an important, but not exclusive part of the whole school e-safety provision for children and staff at Brookes UK.

7. **Managing Video Conferencing and Webcam use**

This technology forms an important part of providing remote learning during periods of lockdown caused by Covid-19 or during prolonged absences of pupils for example due to travel restrictions or medical reasons. Guidance for staff and pupils whilst using are given in appendix 3. This guidance will be reviewed and amended as necessary to ensure that full use of these technologies can be made for remote learning whilst ensuring that staff and pupils are kept safe.

8. **Managing emerging technologies**

Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed. The Senior Leadership Team acknowledges that technologies such as mobile phones, tablets and games machines with wireless Internet access can bypass school filtering systems and are aware of the risks this presents. Mobile devices will not be used by children during school lessons or during formal school time unless it forms part of a pupils normal way of working or specific permission has been granted by the Principal. The sending of abusive or inappropriate text messages or images including sexting is forbidden. Adults may use hand held devices and mobile phones responsibly, according to the staff acceptable use of ICT code of practice.

9. **Protecting Personal Data**

Personal data will be recorded, processed, transferred and made available under GDPR regulations, according to the Data Protection Act 2018.

10. **Prevent Duty**

Prevent Risk assessement considers how learners may be susceptible to radicalism into terrorism.

Policy Decisions

1. **Authorising Internet access**
   All staff must read and sign the Brookes UK Acceptable Use Policy (AUP) before using ICT resources. The school will maintain a current record of all those who are granted access to the school ICT systems. At KS1 and KS2 access to the Internet will be with direct supervision. All children will be taught how to make independent and discerning use of the Internet. Parents and children will be asked to sign and return an ICT agreement (see appendix 4) at the beginning of each academic year, without which pupils will not be allowed access to the school's ICT provision. Any person not directly employed by the school e.g. after school providers, will read and sign the AUP and agreement before being allowed to access the internet in school.

2. **Assessing Risks**
   The School takes all reasonable precautions to prevent access to inappropriate content, contact or conduct. However due to the complexity, scale and constantly evolving nature of internet capability and content, it is not possible to guarantee that unsuitable content, contact or conduct will never occur via a computer connected to the school network. The School will not accept liability for any material accessed, or any consequences of Internet access. The School will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate and effective. The School will be vigilant in monitoring and identifying those at risk regarding online safety, especially those more at risk of being groomed or radicalised, such as those who spend significantly more time online, without supervision.

3. **Handling e-safety complaints**
   Complaints of computer or Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Principal. Complaints of a child protection nature will be dealt with through the school Child Protection Procedures. Pupils and parents will be informed of the complaints procedure. Pupils and parents will be informed of consequences for pupils misusing the school computer facilities and/or the Internet. Sanctions for misuse may lead to terminating access temporarily or permanently or, in the case of an adult, may lead to police involvement and/or dismissal.

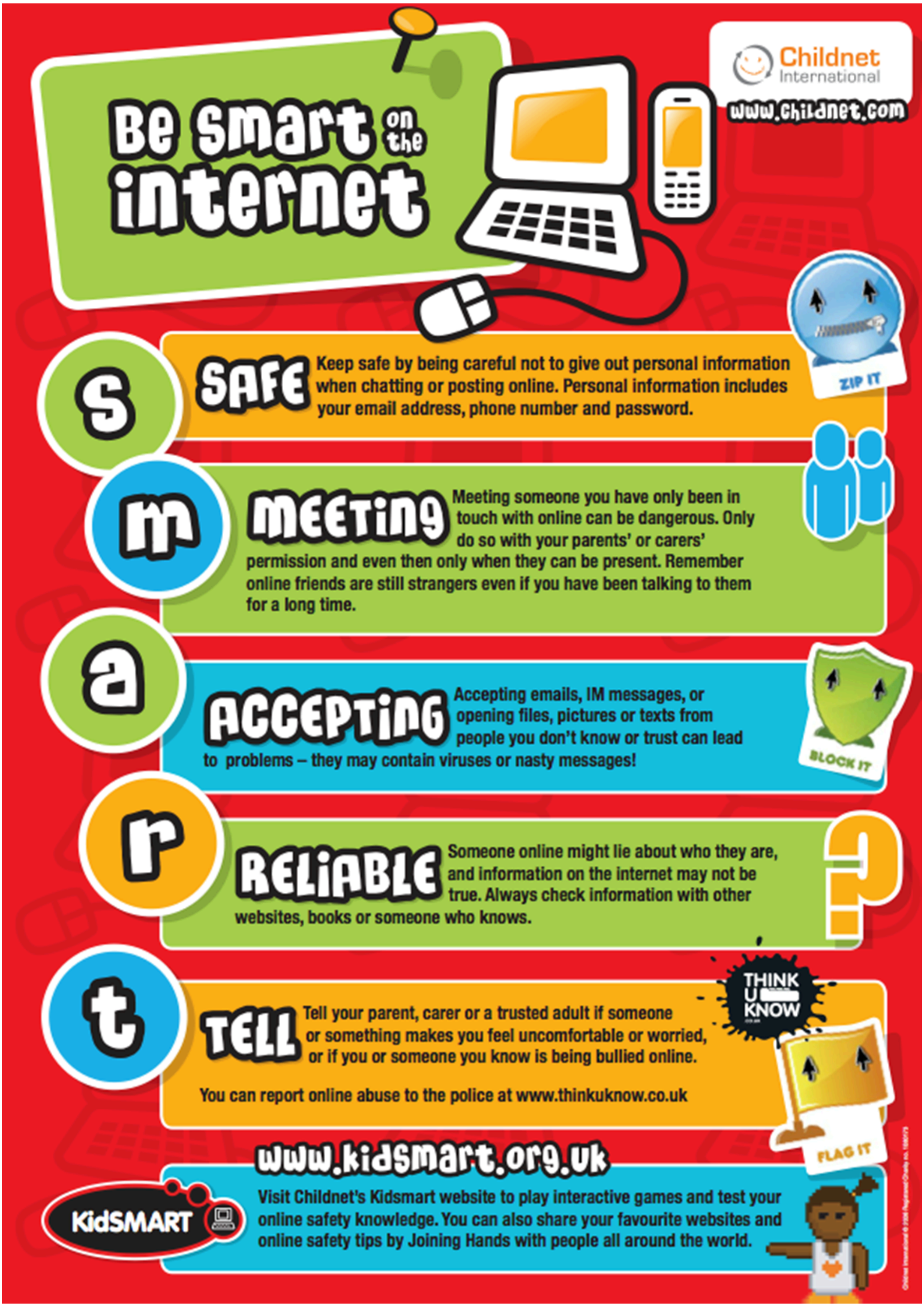
Communications Policy

1. **Introducing the e-safety policy to pupils**
   e -Safety rules, (Appendix 1) will be posted in all rooms where computers are used and discussed with pupils regularly. Pupils will be informed that network and internet use will be monitored and misuse will be appropriately followed up. A programme of e-Safety will be delivered at the start of each year for all pupils, and at stages throughout the year. There will be an e-safety assembly to coincide with e-safety week and throughout the year if issues arise. These will be based on materials from Child Exploitation and Online Protection (CEOP).

2. **Staff and the e-Safety Policy**
   All staff will be given a copy of the e-Safety Policy. All staff will undertake e- safety training through dedicated e-safety staff meetings and as part of the school's planned Child Protection/Safeguarding training.

3. **Enlisting parents' and carers' support**
   Parents' and carers' attention will be drawn to the e-Safety Policy in newsletters, the prospectus and the school website. The School will maintain a list of online e-Safety resources, (appendix 2) along with other "Keeping your child Safe" materials. Each year parents will sign an AUP in respect of their children.

Appendix 1



Be Smart on the internet

S SAFE Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.

T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Appendix 2

Staying safe online

The School provides up-to-date expert information on e-safety shared through the **CEOP** (Child Exploitation and Online Protection Centre) and **Parent Zone** (parentzone.org.uk) to help ensure that children stay safe online.

Parents and children are invited to review the materials to learn more about how to stay safe online at the CEOP and Parent Zone websites.

https://parentzone.org.uk

https://www.ceop.police.uk/safety-centre/

Appendix 3

Remote Teaching and Learning (online)

1. Why consent is required?

- Consent is required to give parents the choice to allow live online video conferencing with their child.
- In response to COVID-19 and to ensure that teachers can engage with students in a safe and secure environment, Brookes UK have made live video available between teachers and students and enabled video for all students and staff inside the Bookes GSuite domain with Brookes GSuite accounts.
- Live video conferencing is **not compulsory** for staff or students. It should be included as one of the methods available for teaching and learning when students and staff are remote from the school environment.

2. Platform choice for video conferencing

- Brookes UK has approved Google Hangouts Meet for live video conferencing and this platform has been tested by Brookes UK.
- Some functions such as live recording and one to one messaging (Chat) have been disabled for safeguarding and privacy reasons.

3. When should Brookes UK teachers use live video conferencing?

- There are academic, social and wellbeing benefits for students and staff in using video conferencing software to communicate and collaborate online.
- Students can connect with their class and teachers when they are learning from home or in other remote locations.
- Brookes UK are aware that not all students and teachers will be able to connect to live video due to limited internet service (bandwidth) or access to digital learning devices.

4. Guidelines for using live online video conferencing

- Pre-recorded lessons and live sessions can be helpful, but they are not compulsory.
- Only whole class or group sessions are allowed.
- Teachers must not conduct 1:1 video or audio sessions with a student.
- Parents will ensure that students understand the guidelines in this document and privacy laws which serve to protect them and Brookes UK staff.

- Parents can help students set up devices, but should not join any live online video or audio conference being delivered by the teacher unless requested to do so by the teacher.

- At the end of any live online video conference between staff and students, students must leave the conference before the teacher closes the session. This ensures that students do not continue chatting without the teacher present.

- Live online video conferencing lessons should be kept as short as possible. A guideline maximum of 30-40 minutes is advised.

- The use of live online video conferencing is one of several options. Teachers can also make use of email, Google Classroom, sending home hard copies of work, using shared documents via Google Drive to communicate and interact with students if they choose.

- The Brookes UK Behaviour Policy applies to all teaching and learning provision.

- Any live online video conference should be regarded as a school lesson and the same school behaviour and discipline policies should apply in this environment.

- Do not allow any unauthorised access to the live online video conference or the area in which it takes place. This includes parents, unless they have been authorised to attend by the teacher prior to the class.

- Students video feeds MUST be ON at all times. The Teacher has the ability to remove a student from the live online video conference if they do not adhere to these guidelines.

- Audio feeds must be enabled at the start of all online live video conferences. Further disabling and enabling of the audio functionality will be at the request of the teacher only.

5. Teacher and student privacy protection

- Teachers and students should only sit in an area with a 'neutral' background. Themed backgrounds serve only to distract. Blurring is now available with Google Hangouts Meet.

- Bedrooms MUST NOT be used to conduct or take part in any Brookes UK live online video conference.

- Teachers delivering live online video lessons have the ability terminate a student’s connection if they think it is right to do so.

Appendix 3

Senior School Student Acceptable ICT Use Agreement

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students* to agree to be responsible users.

Acceptable Use Agreement

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

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password.
- I will only use my school accounts to log on to devices.
- I will be aware of “stranger danger”, when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

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

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

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

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

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

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

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

Please sign & date the agreement form to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign, access will not be granted to school systems and devices.

Lower School - KS2 Student Acceptable ICT Use Agreement

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students* to agree to be responsible users.

Acceptable Use Agreement

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

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password.

- I will only use my school accounts to log on to devices.
- I will be aware of “stranger danger”, when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

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

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

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

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

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

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

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

Please sign & date the agreement form to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign, access will not be granted to school systems and devices.

Lower School - KS1 Student - Acceptable ICT Use Agreement

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe whilst using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students* to agree to be responsible users.

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child):

Signed (parent):