| Policy | Online Safety and Acceptable Use Policy 2022-2023 |
|---|---|
| **Author/Person Responsible** | *Helen Porter*<br>*Headteacher* |
| **Date of Ratification** | *27 September 2022* |
| **Review Group** | *Quality of Education KFPS* |
| **Ratification Group** | *FGB* |
| **Review Frequency** | *Annually* |
| **Review Date** | *September 2023* |
| **Previous Review Amendments/Notes** | |
| **Related Policies** | *Child Protection Policy*<br>*Anti-Bullying Policy*<br>*Behaviour Policy* |
| **Chair of Governors Signature** |  |

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, in school, and also out of school where actions relate directly to school-set activity or use of school online systems. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site. This is pertinent to incidents (such as cyber-bullying) which may take place out of school but are linked to membership of the school. The school will deal with such incidents according to this policy and associated behaviour and anti-bullying policies, and will inform parents/carers of known incidents of inappropriate Online safety behaviour that take place out of school.

It is the school's responsibility to ensure children are safe from terrorist and extremist material when accessing the internet in school. The school will ensure that suitable filtering is in place and will play an important role in equipping children and young people to stay safe online, both in school and outside.

The school recognises that some factors can make children and young people more vulnerable to abuse (NSPCC 2022):

- Age: Pre and early teens are especially vulnerable age for children online
- Gender: Boys and girls may differ in the types of risks they take online and the risks they are exposed to.
- Loneliness, social isolation and family problems may make young people more vulnerable to be groomed online.
- SEN/D: Children with special educational needs or disability are particularly vulnerable to online abuse.

The following sections outline the roles and responsibilities, policy statements and education relating to Online safety for individuals and groups within the school.

1. **Roles and Responsibilities**

1.1. These are clearly detailed in Appendix 1 for all members of the school community.

1.2. The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for Online safety is delegated to the Online safety Co-ordinator.

1. Online Line Safety Lead: Helen Porter, Headteacher
2. Online Safety Curriculum Leads: Craig Black and Michelle Walker
3. Safeguarding Governor: Carol Warrant

1.3. The designated person for child protection is trained in online safety issues and is aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults/strangers, or potential or actual incidents of grooming and cyber-bullying.

2. **Staff and Governors**

2.1. There is a planned programme of Online safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this and the acceptable use policies.

2.2. All new staff receive Online safety training as part of their induction programme.

2.3. The Online safety curriculum lead receives regular updates government updates, and by reviewing regular Online safety updates from the local authority.
2.4. The Online safety Lead provides advice/guidance and training to individuals and seeks LA advice on issues, where required

3. **Pupils**

3.1. Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of pupils in online safety is therefore an essential part of our 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.
3.2. There is a planned online safety programme.
3.3. Key online safety messages are reinforced through an assembly and class work.
3.4. Pupils are helped to understand the pupils' acceptable use policy and act accordingly.
3.5. Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
3.6. Staff act as good role models in their own use of computing equipment.

4. **Curriculum**

4.1. Online safety is a focus in all relevant areas of the curriculum.

4.2. In lessons where internet use is planned, pupils are guided to sites checked as suitable for their use, and processes are in place for dealing with any unsuitable material that is found in internet searches.
4.3. Where pupils are allowed to search the internet freely, staff are vigilant in monitoring the content of the websites the young people visit, and encourage students to use specific search terms to reduce the likelihood of coming across unsuitable material.
4.4. Pupils are taught to be critically aware of the materials and content they access on-line and to assess the accuracy of information (including 'fake news').
4.5. Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
4.6. Pupils will use and apply SMART rules when online. S (Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password). M (Meeting someone you have only been in touch with online can be dangerous. Only do so with your parent's or carer's 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 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 (Someone online might lie about who they are and information on the internet may not be true or reliable. Always check information with other websites, books or someone who knows. If you like chatting online, it's best to chat only to your real-world friends and family). T (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).
4.7. Pupils with SEN have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. Teachers/ TAs will

work closely with these pupils to ensure they have a developed understanding of how to keep safe online.

4.8. The school will send home personal log ins and accounts for children to access some websites from home. These will be checked and approved by the Online Safety Lead and deemed appropriate to support engagement and learning. These websites include but are not limited to: Times Tables Rock Stars, Freckle.

5**. Remote learning:**

5.1. In the event of an incident where remote learning needs to be activated, the school has capacity to do this through the use of Class Dojo.

5.2. Any videos of teachers must be uploaded to the secure, Class Dojo website and not to public forums such as YouTube. Videos of teachers must be pre-recorded and checked to ensure no inappropriate words, noises or actions can be seen/heard before being uploaded.

5.3. Live sessions: If Google Teams or Zoom is being used for 'live' sessions, they must be recorded to safeguard teachers and children. The 'learning objective' or specific intention for the session must be clear and shared with parents, children and staff prior to the live session and the session must not stray from the designated topic.

6. **Parents / Carers**

6.1. Parents and carers may have only a limited understanding of online safety issues and may be unaware of risks and what to do about them; however they have a critical role to play in supporting their children with managing online safety risks at home, reinforcing key messages about online safety and regulating their home experiences. The school supports parents to do this by:

- providing clear Acceptable Use Policy guidance, newsletter and web site updates
- providing an awareness-raising meeting for parents

7. **Technical Staff - Roles and Responsibilities**

7.1. Technical support is provided by Integra Service Desk (01454 863838).

7.2. Integra provides technical guidance for online safety issues, and the team is fully informed about the issues. Where Integra provides technical support, the "administrator" passwords for the school are not held by the school and the local authority is responsible for their security and any implications of their use.

7.3. The school ensures, when working with our technical support provider, that the following guidelines are adhered to:

- School computer systems are managed in ways that ensure that the school meets the online safety technical requirements.
- There are regular reviews of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems.
- All users are provided with a username and password by the technical support provider.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any evidence or suspicion that there has been a breach of security.

7.4.The school upholds and supports the managed filtering service provided Integra
7.5.In the event of the school technician needing to make requested changes to filtering, or for any user, this is logged and carried out by a process that is agreed by the Headteacher.
7.6.Any filtering issues are reported immediately to the Integra technical team.
7.7.School ICT technical staff regularly monitor and record the activity of users on the school's ICT systems and users are made aware of this in the Acceptable Use Policy.
7.8.Actual and potential online safety incidents are documented and reported immediately to the Online safety Leader who will arrange for these to be dealt with immediately in accordance with the acceptable use policy.
7.9.Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc. from accidental or malicious attempts which might threaten the security of the school's systems and data.
7.10.The provision of temporary access for "guests" (e.g. trainee teachers, visitors, supply teachers) to the school system must be approved and completed by the technical support provider.
7.11.Only teaching and administrative staff are allowed to download executable files and these must be for educational purposes.
7.12.Teaching and administrative staff are allowed to use laptops and other portable devices assigned to them out of school for personal use. The laptops and other portable devices are for their sole personal use only and should be used in accordance with the guidelines set out in this policy and other related policies. Laptops and other portable devices assigned to pupils can be used out of school for educational use only (see the GDPR section for further detail).
7.13.Teaching and administrative staff only can request programmes to be installed on school workstations/portable devices but this must be approved and completed by the technical support provider.
7.14.wherever possible USB sticks are not used however, in some circumstances, this may be permitted by requesting to use them from SLT eg. For interviews / visitors, every effort should be made to ask them to email items in advance.
7.15.The school infrastructure and individual workstations are protected by up to date virus software.
7.16.The school infrastructure and individual workstation software are updated by the school's technical support provider.
7.17.The school infrastructure and individual workstation security updates/patches for the operating system are kept up to date by the school's technical support provider.
7.18. Personal data may be sent using school outlook so long as it is to another South Glos email address or secure provider such as the NHS.

8. **Use of digital and video images**

8.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are reported incidents of employers carrying out internet searches for information about potential and existing employees. The school

informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm.

8.2. When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images, including on social networking sites.

8.3. Staff are allowed to take digital/video images to support educational aims, but follow guidance in the Acceptable Use Policy concerning the sharing, distribution and publication of those images.

8.4. Staff ensure that pupils also act in accordance with their Acceptable Use Policy.

8.5. Pupils' work is only published on a public web site with the permission of the pupil and parents or carers.

8.6. We do not use publicly accessible webcams in school

8.7. Webcams in school will only be used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults. Webcams are also used for assemblies and other cross school gatherings. When children are on webcam, it must be using the school's internal internet. Misuse of the webcam by any member of the school community will result in sanctions.

9. **General Data Protection Regulation (GDPR)**

9.1. Storage of all data within the school will conform to the UK data protection requirements and subsequent General Data Protection Regulation (GDPR). Refer to GDPR Policy

9.2. Staff must ensure that they:

- take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- use personal data only on secure password-protected computers and other devices, ensuring that they are properly logged off at the end of any session in which they are using personal data;
- restrict the storage of school-related personal data to school equipment (including computers and portable storage media);
- transfer data using encryption and secure password-protected devices;
- when personal data are stored on any portable computer system, USB stick or any other removable media;
- the data must be encrypted and password-protected;
- the device must be protected by a password plus virus and malware checking software (many memory sticks/cards and other mobile devices cannot be password protected and therefore should not be used);
- the data must be securely deleted from the device once it has been transferred or its use is complete.

10. **Guidance on the Use of Communications Technologies**

10.1. A wide range of communications technologies have the potential to enhance learning.
10.2. The official school email service is used for communications between staff and with parents/carers and pupils, as it provides an effective audit trail.
10.3. Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
10.4. Users are made aware that email communications may be monitored and are informed through the Acceptable Use Policies of what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
10.5. Personal information is also not posted on the school website and only official email addresses are listed for members of staff.

11. **Social media**

11.1. Staff must not, under any circumstances, accept pupils as 'friends' and must not approach pupils to become their friends on social networking sites. Personal communication of this nature could be considered inappropriate and unprofessional, and make that individual vulnerable to allegations.
11.2. Any pupil-initiated communication, or online friend requests, must be declined and reported to the Headteacher.
11.3. Staff should not be online friends with ex or recent pupils of the school or other schools.
11.4. They should not share any personal information with any pupil, including personal contact details, personal website addresses or social networking site details.
11.5. If staff are online 'friends' with any parent/carer linked with the school, they must ensure that they do not disclose any information or otherwise post details which may bring themselves or the school into disrepute. Staff must not engage in any online discussion about any child attending the school.
11.6. School staff must not disclose, on any social networking site, any information that is confidential to the School, Governing Body, or Local Authority, or post anything that could potentially bring the School, Governing Body or Local Authority into disrepute.
11.7. They must not disclose any personal data or information about any individual/colleague/pupil, which could be in breach of the GDPR.
11.8. Staff should not post photographs of pupils under any circumstances, and should not post photographs of colleagues or others in the school community without their express permission.
11.9. Care should be taken to avoid using language which could be deemed offensive to others.
11.10. Staff must take steps to ensure their online personal data are not accessible to anybody they do not wish to access them. For example, they are advised to check the security and privacy settings of any social networking site they subscribe to and set these to maximum.

11.11. If staff notice inflammatory comments or posts that will bring the school into disrepute during their regular use of social media, they should report it to the Headteacher or DSL.

11.12. The following table shows how the school currently considers these should be used.

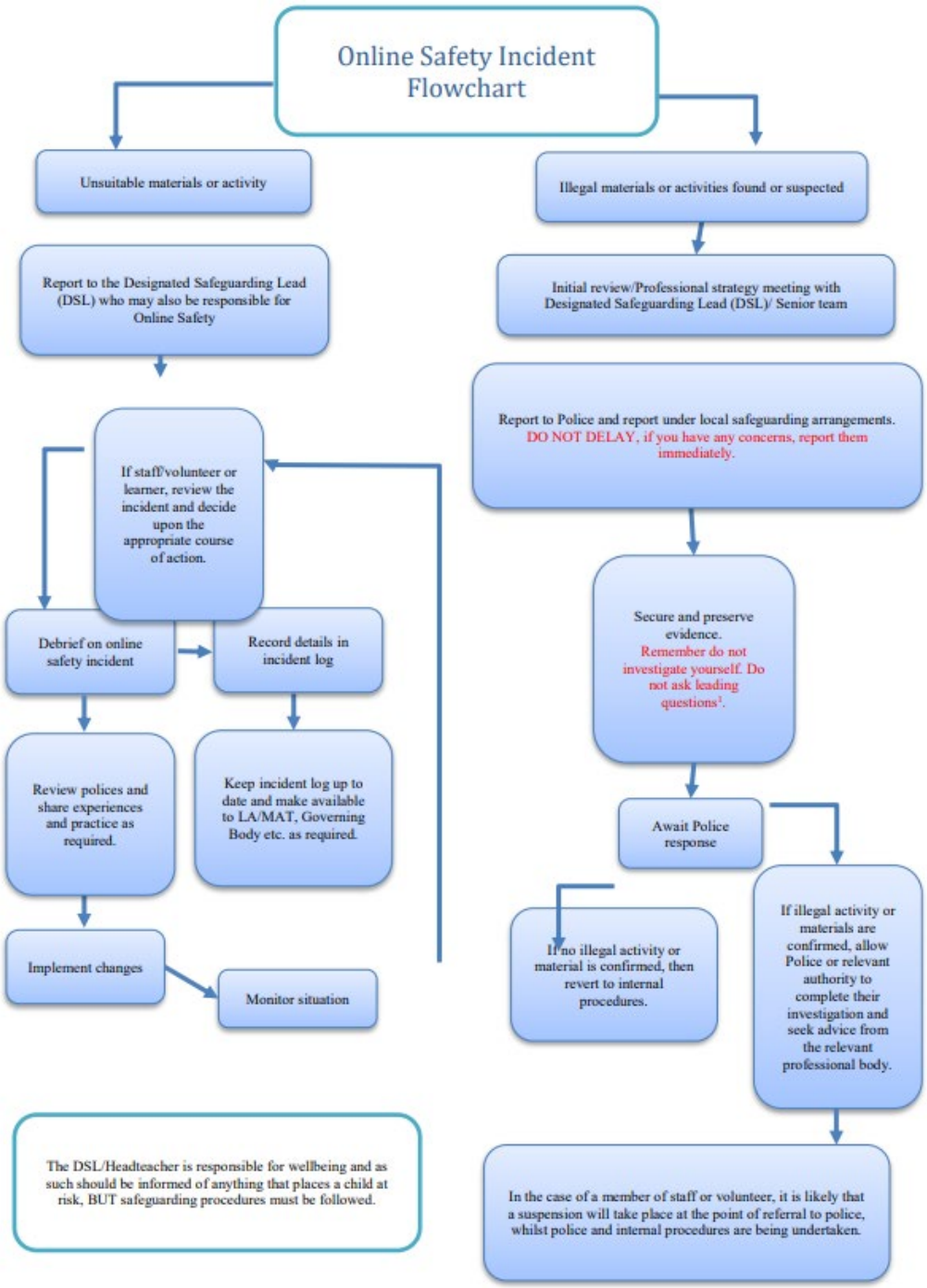
| | Staff & other adults | | | | Students / Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | X | | | | | | X | |
| Use of mobile phones in lessons | | | | X | | | | X |
| Use of mobile phones in social time | X | | | | | | | X |
| Taking photos on mobile phones or other camera devices | | | | X | | | | X |
| Use of personal gaming devices | | | | X | | | | X |
| Use of personal email addresses in school, or on school network | | | | X | | | | X |
| Use of school email for personal emails | | | X | | | | | X |
| Use of open chat rooms / facilities | | | | X | | | | X |
| Use of school limited chat facilities | X | | | | X | | | |
| Use of public instant messaging | | | | X | | | | X |
| Use of instant messaging across the school community | X | | | | | X | | |
| Use of social networking sites | | | X | | | | | X |
| Use of moderated social networking sites only across the school community | | | | X | | | | X |
| Use of blogs | X | | | | | | X | |
| Use of moderated blogs only across the school community | X | | | | | | X | |

**Responding to incidents of misuse**

We expect all members of the school community to be responsible users of computing equipment who understand and follow this policy. However, there may be times when infringements of the policy occur through careless, irresponsible or, very rarely, deliberate misuse. If any apparent or actual misuse appears to involve illegal activity, the flow chart below is consulted and followed, in

particular the sections on reporting the incident to the police and the preservation of evidence. Illegal activity would include:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials



If members of staff suspect that any misuse might have taken place, it is essential that correct procedures be used to investigate in a proportionate manner, and that members of the school community, police (if necessary) be made aware that incidents have occurred and are being dealt with.

**Unsuitable / inappropriate activities**

The school believes that the activities referred to below are inappropriate in a school context and that users should not engage in these activities in school, or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | child sexual abuse images | | | | | X |
| | promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation | | | | | X |
| | adult material that potentially breaches the Obscene Publications Act in the UK | | | | | X |
| | criminally racist material in UK | | | | | X |
| | pornography | | | | X | |
| | promotion of any kind of discrimination | | | | X | |
| | promotion of racial or religious hatred | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | any other information which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |
| Using school systems to run a private business | | | | | X | |
| Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school | | | | | X | |
| Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions | | | | | X | |
| Revealing or publicising confidential or proprietary information (e.g. financial / personal, databases, computer / network access codes and passwords) | | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | | X | |

| | | | | | |
|---|---|---|---|---|---|
| Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet | | | | X | |
| On-line gaming (educational) | | X | | | |
| On-line gaming (non educational) | | | | X | |
| On-line gambling | | | | X | |
| On-line shopping / commerce | | | X | | |
| File sharing | | | | X | |
| Recreational use of Social Networking during directed time (staff) | | | | X | |
| Use of social networking sites apart from where sanctioned for specific educational use by Headteacher | | | | X | |
| Use of video broadcasting e.g. Youtube | | | X | | |

## Appendix 1 Roles and Responsibilities

| | |
|---|---|
| Governors | • Approve and review the effectiveness of the Online safety Policy and acceptable use policies;<br>• Safeguarding Governor works with the Online safety co-ordinator to carry out regular monitoring of Online safety incident logs, filtering, changes to filtering, and then reports to Governors. |
| Head teacher and Senior Leaders | • Ensure that all staff receive suitable CPD to carry out their Online safety roles and that sufficient resources are allocated;<br>• Ensure that there is a system in place for monitoring Online safety;<br>• Follow correct procedure in the event of a serious Online safety allegation being made against a member of staff;<br>• Inform the local authority of any serious Online safety issues including filtering;<br>• Ensure that the school infrastructure/network is safe and secure and that policies and procedures approved within this policy are implemented. |
| Online safety Lead | • Take a leading role in establishing/reviewing Online safety policies/documents;<br>• Ensure all staff are aware of the procedures outlined in policies;<br>• Provide and/or broker training and advice for staff;<br>• Attend updates and liaise with the Integra Online safety staff and technical staff;<br>• Deal with and log Online safety incidents;<br>• Meet with Safeguarding Governor regularly to discuss incidents and review the log;<br>• Report regularly to Senior Leadership Team. |
| Teaching and Support Staff | • Participate in any training and awareness raising sessions;<br>• Have read, understood and signed the Staff Acceptable Use Agreement (AUP);<br>• Act in accordance with the AUP and Online safety Policy;<br>• Report any suspected misuse or problem to the Online safety Co-ordinator;<br>• Monitor ICT activity in lessons, extracurricular and extended school activities; |

| | |
|---|---|
| Pupils | • Participate in Online safety activities, follow the Acceptable Use Policy and report any suspected misuse;<br><br>• Understand that the Online safety Policy covers actions out of school that are related to their membership of the school. |
| Parents and carers | • Ensure that their child/children follow acceptable use rules at home;<br>• Discuss Online safety issues with their child/children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet;<br>• Access the school website in accordance with the relevant school Acceptable Use Policy;<br>• Keep up to date with issues through school updates and attendance at events. |
| Technical Support Provider | • Ensure the school's ICT infrastructure is secure in accordance with South Gloucestershire guidelines and is not open to misuse or malicious attack;<br>• Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data;<br>• Inform the Headteacher of issues relating to filtering;<br>• Keep up to date with Online safety technical information and update others as relevant;<br>• Ensure use of the network is regularly monitored in order that any misuse or attempted misuse can be reported to the Online safety Co-ordinator for investigation/action/sanction;<br>• Ensure monitoring software/systems are implemented and updated.<br>• Ensure all security updates/patches are applied (including up to date antivirus definitions, Windows updates) and that reasonable attempts are made to prevent spyware and malware. |
| Community Users | Sign and follow the AUP before being provided with access to school systems. |

**Kings Forest Primary School Rules for Keeping Safe with ICT Key Stage 1**

- I will ask a teacher when I want to use the computer or contact people using ICT.
- I will use a computer only when an adult is present.
- I will use only the web sites that I am allowed to.
- I will keep my password secret and not tell it to anyone.
- I will be polite and friendly when I use the computer to contact people.
- I will keep my personal details secret and not tell anybody about my home, family and pets. I will keep my friends' details secret too.
- I know that things I put up on the internet can be seen by anyone and I will not upload anything without asking an adult first.
- I will not take or share pictures of anyone without asking them first.
- I will check information I find online, as it might not be true.
- I know that I should not buy anything on line.
- I will tell a teacher (or adult I trust) if I find anything on a computer or a message that is mean, upsetting or worrying.
- I will tell a teacher (or adult I trust) if I know of anyone who is behaving badly on line or if I know anyone may be being bullied.
- I will use ICT by these rules when:
- I use school computing equipment.
- I use my own computing equipment out of school for school activities.
- If I deliberately break these rules then I know that there will be consequences.

My Name is

My Class teacher is

Signed

Date

**Kings Forest Primary School Primary School Key Stage 2 - Rules for Keeping Safe with ICT**

Content

- I will use clear search words so that I find the right information.
- I know that some content may not be filtered out and what to do if I find something worrying.
- I will double check information I find online.

Contact

- I know that I need to behave well online as in real life and be polite and friendly.
- I will not open messages if the subject field is not polite or if I do not know who they are from.
- I am careful about what I send as messages can be sent on to my parents or headteacher.
- I know that I must have permission to communicate online and will make sure my teacher/ parents know who I communicate with.
- I will talk to an adult if an online friend wants to meet me and will never arrange to meet anyone without permission.
- I know that anything I put up on the internet can be seen by anyone.
- I will only use my mobile phone at school for things that the school allows.

Conduct

- I will not use computing equipment in school without permission from my teacher.
- I will choose my user names and passwords carefully to protect my identity and I will not share them. I will not ask computers to remember my password.
- I know I must keep my personal details and those of others private.
- I will not attempt to visit unsafe sites or register for things I am not old enough for.
- I will log off sites when I have finished.
- I know that I should not buy anything on line without permission.
- I will not use anyone else's work or files without permission.
- Where work is protected by copyright, I will not try to download copies.
- I will not take or share pictures of anyone without their permission.

Problems

- I will not try to change computer settings or install programmes.
- I will not damage equipment and will tell a teacher if equipment is broken or not working.
- I will tell a teacher or adult I trust if I find anything on a computer or a message that is unpleasant or makes me feel uncomfortable.
- I will tell a teacher or adult I trust if I know of anyone who is behaving badly on line or anyone who may be being bullied.
- I agree to use ICT by these rules when:
  - I use school ICT or my own in school (including my mobile phone when allowed).
  - I use my own ICT (including mobile phone) out of school to access school sites or for school activities.

I understand that if I break these rules there could be the following consequences:

| | |
|---|---|
| My Name is | |
| My Class teacher is | |

| | | | |
|---|---|---|---|
| Signed | | Date | |