PENNYHILL PRIMARY SCHOOL

ONLINE SAFETY POLICY

1. Introduction

This Online Safety policy recognises the commitment of our school to keeping staff and pupils safe online and acknowledges its part in the school's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The Online Safety Policy supports this by identifying the risks and the steps we are taking to avoid them. The breadth of issues classified within online safety is considerable, but can be 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
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm (DfE Keeping Children Safe in Education Jan 2021)

This policy shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

Our expectations for responsible and appropriate conduct are set out in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.
As part of our commitment to Online Safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets from loss or inappropriate use.

The scope of this policy

This policy applies to the whole school community including the Senior Leadership Team (SLT), Governing Body (GB), all staff employed directly or indirectly by the school, visitors and all pupils.

The Senior Leadership Team and school governors will ensure that any relevant or new legislation that may impact upon the provision for online safety within school will be reflected within this policy.

The person in school taking on the role of Online Safety lead is

Michelle Williams with support from the Computing Coordinator

The Governor with an overview of Safeguarding, including online safety:

Jackie Ranger

The policy written: December 2020

Implementation of the policy

The Senior Leadership Team will ensure all members of school staff are aware of the contents of the school Online Safety Policy and the use of any new technology within school.

All staff and pupils will sign the relevant Acceptable Use Policies

All amendments will be published and awareness sessions will be held for all members of the school community.

Online safety will be taught as part of the curriculum in an age-appropriate way to all pupils.

Online safety posters will be prominently displayed around the school.

The Online Safety Policy will be made available to parents, carers and others via the school website.

2. Responsibilities of the School Community

We believe that online safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The senior leadership team accepts the following responsibilities:

- The Headteacher will take ultimate responsibility for the online safety of the school community
- Identify a person (the Online Safety Lead) to take day to day responsibility for online safety; provide them with training; monitor and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the governors
- Develop and promote an online safety culture within the school community
- Ensure that all staff, pupils and other users agree to the Acceptable Use Policy and that new staff have online safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to online safety
- Receive and regularly review online safety incident logs, via CPOMS notifications; ensure that the correct procedures are followed should an online safety incident occur in school and review incidents to see if further action is required

Responsibilities of the Online Safety Lead

- Promote an awareness and commitment to online safety throughout the school
- Create and maintain online safety policies and procedures
- Develop an understanding of current online safety issues, guidance and appropriate legislation through regular training
- Ensure delivery of an appropriate level of training in online safety issues
- Ensure that online safety education is embedded across the curriculum
- Ensure that online safety is promoted to parents and carers
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident
- Ensure that posters for online safety are displayed in classrooms and around the school
- To ensure that the school Online Safety Policy and Acceptable Use Policies are reviewed regularly

Responsibilities of the Headteacher

- Take day to day responsibility for online safety within the school
- Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
-

Responsibilities of all Staff

- Read, understand and help promote the school's online safety policies and guidance
- Read, understand and adhere to the staff AUP
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that all digital communication with pupils is on a professional level and only through school based systems, **NEVER** through personal email, text, mobile phone social network or other online medium (see Code of Safer Practice, Code of Conduct)
- Embed online safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all online safety incidents to the Headteacher

Additional Responsibilities of Technician and SBM

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps, including filtering and monitoring, are in place to safeguard the security of the school IT system, sensitive data and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and detection and prevention of malicious attack
- Report any online safety related issues that come to their attention to the Headteacher
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the schools IT equipment
- Liaise with the Local Authority, internet providers and others as necessary on online

safety issues
- Document all technical procedures and review them for accuracy at appropriate intervals
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

Responsibilities of Pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance
- Take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff
- Discuss online safety issues with family and friends in an open and honest way
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices
- To know, understand and follow school policies regarding online bullying

Responsibilities of Parents and Carers

- Help and support the school in promoting online safety
- Read, understand and promote the pupil AUP with their children
- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology
- To agree to and sign the Online Safety Agreement containing a statement regarding their personal use of social networks in relation the school:

We will support the school's approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

Responsibilities of the Governing Body

- Read, understand, contribute to and promote the school's online safety policies and guidance as part of the school's overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for the school to implement the online safety strategy.

3. Acceptable Use Policies

School has a number of AUPs for different groups of users. These are shared with all users yearly and staff and pupils will be expected to agree to them and follow their guidelines. We will ensure that external groups and visitors to school who use our ICT facilities are made aware of the appropriate AUP.

School Acceptable Use Policy documents

- AUP EYFS Pupil
- AUP KS1 Pupil
- AUP KS2 Pupil
- AUP Staff

4. Training

Technology use changes at a fast pace, and we recognise the importance of regular staff training. All school staff will receive regular updates on risks to pupils online from the Online Safety Lead, and attend online or external training as necessary.

5. Teaching and Learning

We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We deliver a planned and progressive scheme of work to teach online safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity. Online safety is taught in specific Computing and PSHE lessons and also embedded across the curriculum, with pupils being given regular opportunities to apply their skills.

We teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

We discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

We will remind pupils about the responsibilities to which they have agreed through the AUP. Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

6. How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.
To achieve this we will offer opportunities for finding out more information through meetings, the school newsletter and website.
We will ask all parents to discuss the pupil's AUP with their child and complete a forms questionnaire (or a paper copy if lack of technology available to access Forms)
We request our parents to support the school in applying the Online Safety Policy.

7. Managing and Safeguarding IT systems

The school will ensure that access to the school IT system is as safe and secure as reasonably possible.
Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.
All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff e.g. head teacher and member of technical support.
The wireless network is protected by a secure log on which prevents unauthorized access.

We do not allow anyone except technical staff to download and install software onto the network.

Filtering

In order to be compliant with the Prevent Duty and Keep Children Safe in Education 2021, the school will:

- Ensure that all reasonable precautions are taken to prevent access to illegal and extremist content. Web filtering of internet content is provided TRUSTnet;
- Inform all users about the action they should take if inappropriate material is accessed or discovered on a computer. Deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.
- Expect teachers to check websites they wish to use prior to lessons to assess the suitability of content.
- Post notices in classrooms and around school as a reminder of how to seek help.

Monitoring

In order to be compliant with the Prevent Duty and Keeping Children Safe in Education 2021, the school will:

- Pupils are always supervised by staff while using the internet as this reduces the risk of exposure to extremist, illegal or inappropriate material; direct supervision also enables school staff to take swift action should such material be accessed either accidentally or deliberately.
- Internet and network use is monitored every week by the SBM to identify access to websites or internet searches which are a cause for concern.
- Daily monitoring is completed by SBM, any concerns reported to Headteacher
- Headteacher is able to access monitoring system.
- Loaned laptops will also have monitoring system. Parental agreements make it explicit that usage is restricted to education purposes only and is monitored daily.

Access to school systems

The school decides which users should and should not have internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third party users.

Passwords

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).
- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.
- All pupils have a unique, individually-named user account and password for access to IT equipment and information systems available within school. Early Years pupils are the exception to this.
- All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They

must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains a log of all accesses by users and of their activities while using the system in order to track any online safety incidents.

Management of assets
All redundant IT equipment is disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Policy written December 2018

Last reviewed on: April 2021

This policy should be read in conjunction with:
- Safeguarding and Child Protection Policy
- Acceptable Use Policy
- Code of Safer Working Practice
- Code of Conduct
- Anti-Bullying Policy
- Mobile Phone Policy
- Twitter Policy
- Information Management Policy (GDPR)

Appendix 1
Acceptable Use Policy for Staff, Governors and volunteers

What is an AUP?

We ask all children, young people and adults involved in the life of Pennyhill Primary School to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually.

Why do we need an AUP?

All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

Where can I find out more?

All staff, governors and volunteers should read Pennyhill's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to Michelle Williams (DSL) or one of the Deputy DSLs

Page Break

What am I agreeing to?

1. (This point for staff and governors): I have read and understood Pennyhill's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead, Michelle Williams, (if by a child) or Headteacher, Elaine Williams, (if by an adult).
1. **During remote learning:**
    - **I will not behave any differently** towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
    - **I will not attempt to use a personal system or personal login for remote teaching** or set up any system on behalf of the school without SLT approval.
    - **I will not take secret recordings or screenshots** of myself or pupils

- **If I notice that the call is being recorded**, I will ask for the recording to be stopped and end the call asking for the recording to be deleted immediately.
- **If the camera is on whilst using Teams, the background can be changed** this will prevent personal information or inappropriate objects being shared.

2. I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.
3. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the **PSHE curriculum,** as well as safeguarding considerations when supporting pupils remotely.
4. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
   - not sharing other's images or details without permission
   - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
8. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and in Pennyhill's social media policy/guidance.
9. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify [insert name/s] if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.
10. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, if allowed, will be encrypted.
11. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education

setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

12. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
13. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
14. I will follow the guidance in the safeguarding and online-safety policies for reporting incident: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
15. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____
Name: _____
Role: _____
Date: _____

Appendix 2
Acceptable Use Policy KS1 pupils

Acceptable use agreement for KS1 children

My name is _____

1. To stay **SAFE online and on my devices**, this is what I will do:	✓.
2. I will only **USE** devices or apps, sites or games if a trusted adult says so	
3. I will **ASK** for help if I'm stuck or not sure	
4. I will **TELL** a trusted adult if I'm upset, worried, scared or confused	
5. If I get a **FUNNY FEELING** in my tummy, I will talk to an adult	
6. I will look out for my **FRIENDS** and tell someone if they need help	
7. I **KNOW** people online aren't always who they say they are	
8. I know that anything I do online can be shared and might stay online **FOREVER**	
9. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to	
10. I don't change **CLOTHES** or get undressed in front of a camera	
11. I always check before **SHARING** personal information	
12. I am **KIND** and polite to everyone	

My trusted adults are:

_____ at school

_____ at home

_____

Acceptable Use Policy KS2 Pupils

These statements can keep me and others safe & happy at school and home

1. ***I learn online*** – I use the school's internet, devices and logons for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. ***I learn even when I can't go to school because of coronavirus*** – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom or nor do teachers. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
5. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
7. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
10. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
11. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
12. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
13. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
14. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
15. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me

worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

16. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
17. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult or skills but very unsuitable.
18. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
19. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
20. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
21. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
22. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult: at school that includes ……..

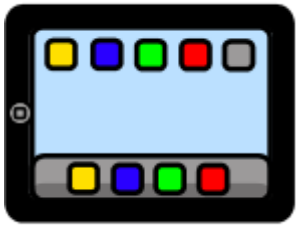
Outside school, my trusted adults are_____

Signed: _____ Date: _____

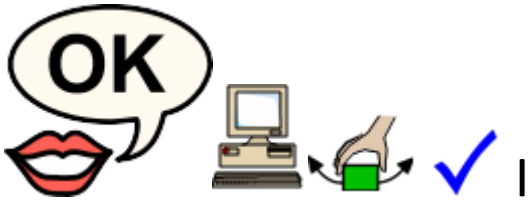
Acceptable Use Policy – SEND children (if needed)

What I Must do to Keep Safe Online and With Devices

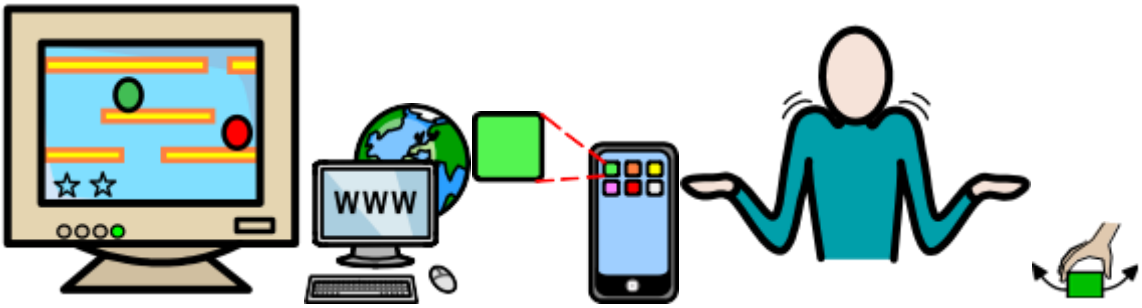
Online means anything connected to the internet. Most devices and apps are connected to the internet.



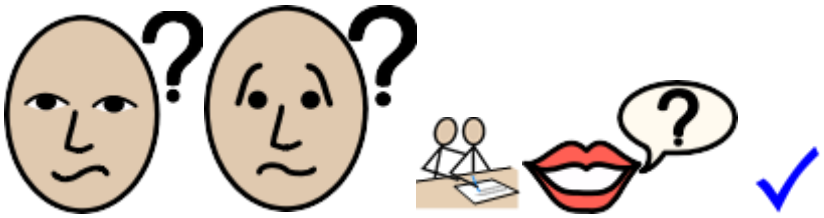
Devices are technology like: computers, laptops, games consoles,
tablets and smart phones.



I will only use the devices I am allowed to use.

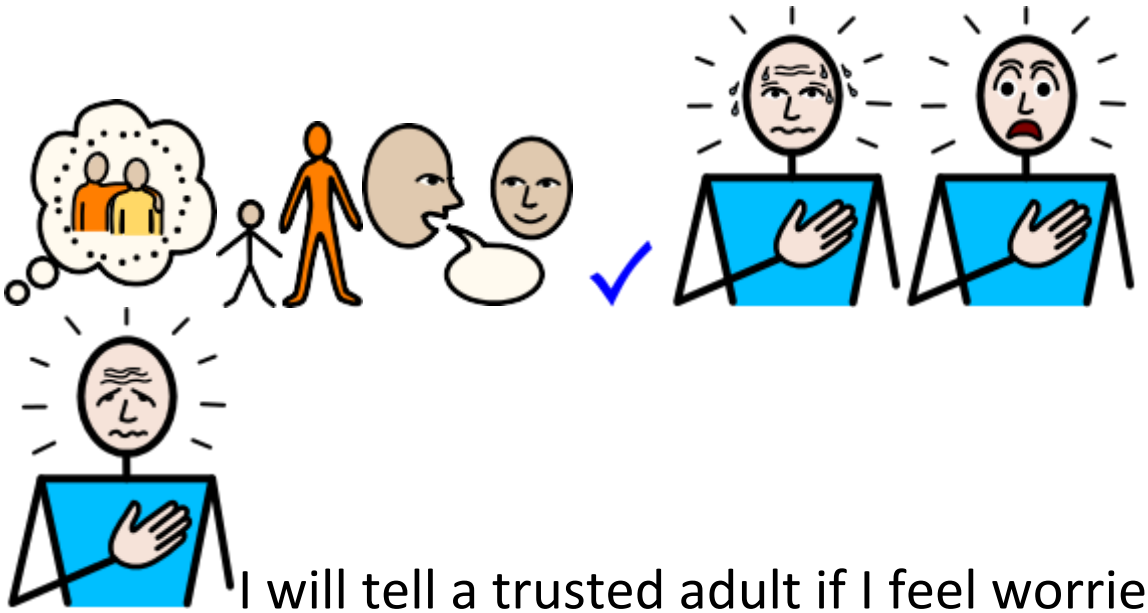


I will ask a trusted adult before I use new websites , games or apps.

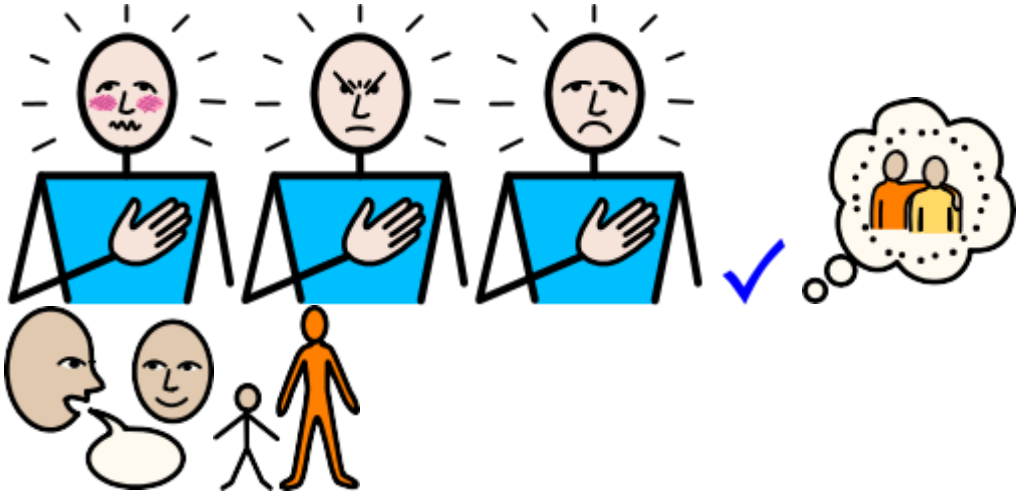


I will ask for help if I'm stuck or not sure.

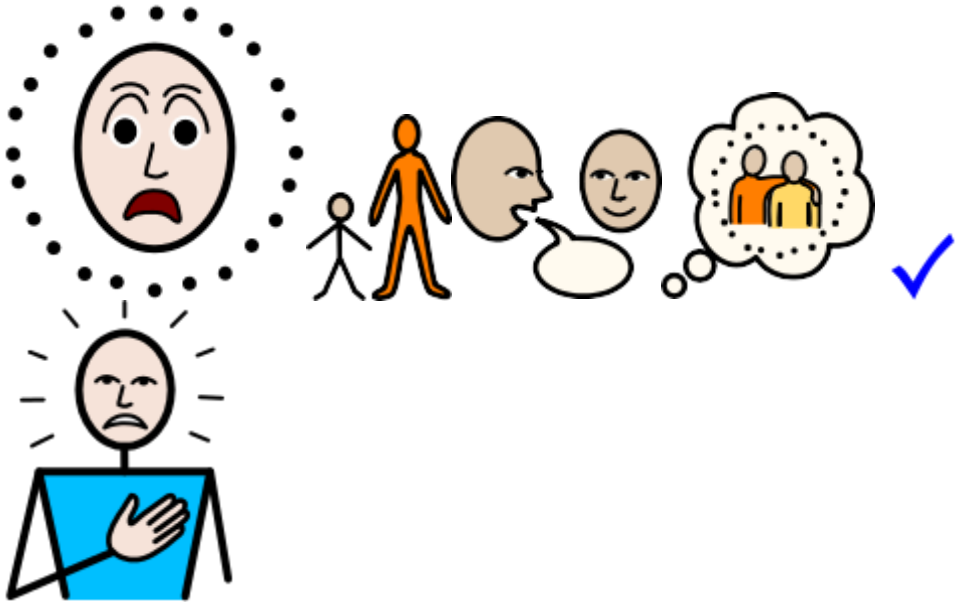
I will be kind and polite to everyone online.



I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.



I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.

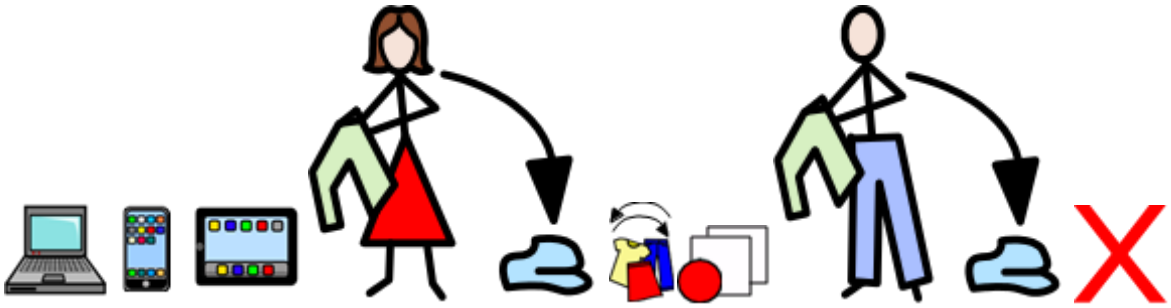


I will tell a trusted adult if I feel bad or unsafe when I am using a device.

I know people online sometimes tell lies.

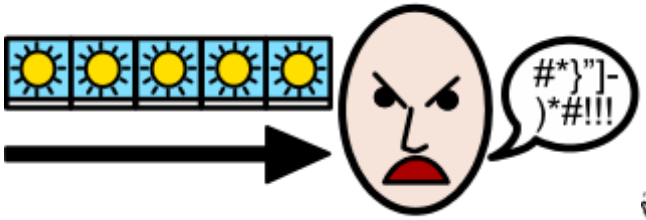
They might lie about who they are or where they live.

I never have to keep secrets from my trusted adults.

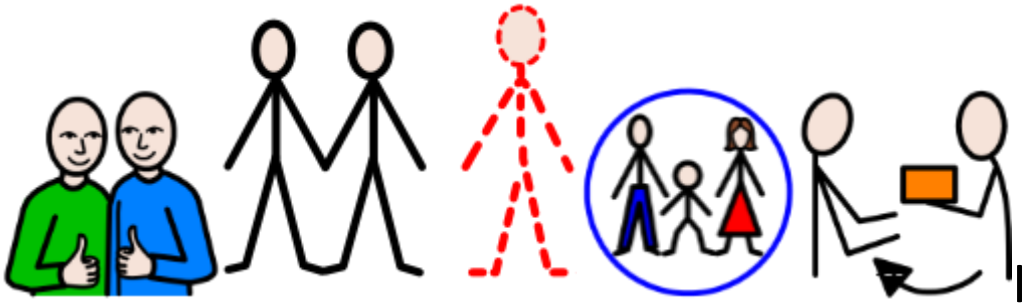


I will not change clothes or undress in front of a webcam.

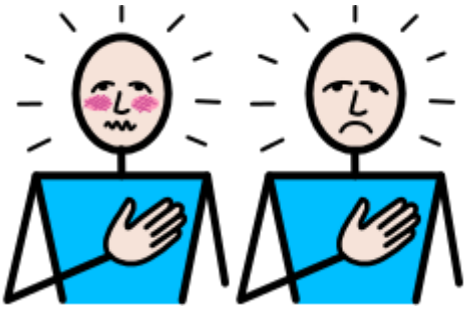
I will always ask a trusted adult before telling anyone my private



information or location.



know that anything I do or say online might stay there forever.

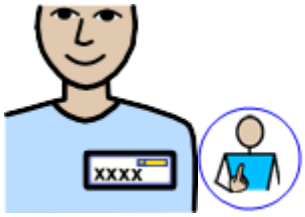


It can be given to my family, my friends or strangers.

This could make me feel sad or embarrassed.

My trusted adults are _____ at scho
ol

My trusted adults are _____ at
home



My name is _____