B70 COMPUTING AND E-SAFETY (ACCEPTABLE USE OF THE INTERNET)

Date of Update	Reason for Update	Next Update
Jan 2024	Annual Review and update to include updates from KCSIE	Jan 2025
Jul 2024	Sharing nudes and semi-nudes: advice for education settings working with children and young people	Jul 2025

Introduction

In a rapidly changing world, the use of Information and Communication Technology is an essential skill for everyday life and to achieve economic well-being. Digital devices can be used to acquire, organise, store, manipulate, interpret, communicate and present information. Norris Bank Primary School recognises that its pupils are entitled to quality hardware and software and a structured and progressive approach to the learning of the skills needed to enable them to use IT effectively. Furthermore, the teaching of IT skills is a statutory requirement of the National Curriculum.
The purpose of this policy is to state how the school intends to make this provision.

Rationale

The school believes that IT helps children to:

- Have immediate access to an endless source of information that is the internet.
- Present information in ways which help them to understand, assimilate and use it more readily.
- Be motivated and enthusiastic learners.
- Focus and concentrate
- Work effectively in a team.
- Learn in an individually appropriate way.

In addition, learning computer science will allow children to:

- Understand how digital systems work and how to put this knowledge into use through programming.
- Become digitally literate. This will allow them not just to use IT to create systems, programs and a range of content but to be critical consumers of such content, understanding how information and images can be manipulated to influence the consumer. This is increasingly important as the use of AI becomes more and more prevalent.

Aims

We aim to produce learners who:

- can become members of the digital generation, confident enough to embrace new developments in technology.
- have met the requirements of the National Curriculum Programmes of Study for IT.
- are able to use IT as a tool to enhance their learning in other areas of the curriculum.
- are not only aware of the dangers inherent in the use of digital technology but of their own responsibilities in keeping themselves and others safe online.

Organisation

The school believes that progress in IT is promoted through regular access and use of technology relevant to a task. The predominant mode of working in IT is as individuals or in small groups although new skills may be introduced to a group of pupils. Practice of skills will occur discreetly while using IT to support work across the curriculum.

Resources, Access and Deployment

- IT network infrastructure and equipment has been provided with an emphasis on the use of an IT suite equipped with 30 Chromeboxes running a cloud-based Google environment.
- 14 classroom machines plus 4 in other locations run Windows 10 Professional Software from a RM server sited in the school. KS2 children also have access to 40 Chrome books in two charging trolleys. All teaching staff and our HLTA also have a touch screen chrome book.

- KS1 and Foundation Stage have access to 30 Chrome books in a charging trolley. These machines also have a touch screen and a more user friendly camera.
- EYFS staff use 5 iPads provided by DfE.
- Additional resources, e.g. A small number of Bbots and Probots, Micro Bits, Robot Mice and Rugged Racers are kept centrally.
- Technical support is provided by AVA services. Problems with IT are reported to AVA through a Google Sheet (AVA Job Reporter) which can be accessed by all school staff.

Planning, assessment, recording and reporting

- The school follows the new IT NC implemented in 2014
- Coding activities form 50% of the curriculum from Year 1-6
- Modules are linked as far as possible to other areas of the creative curriculum to enable IT to be used as a learning tool. School makes use of our PurpleMash subscription for support with planning and assessment.
- Pupil progress towards objectives will be recorded by teachers in digital Year Group assessment folders identifying learners who have met, not met or exceeded learning expectations.
- Pupils either save work within PurpleMash or in Google Classroom which is accessed through a unique Gmail address.
- Google Classroom is the school's preferred remote learning platform.

Equal Opportunities

All children, regardless of gender, ethnicity and needs have equal access to the IT curriculum and have the opportunity to make the most of their own potential within this field.

Coordination, Management and Personnel

- IT is led by a team who meet regularly and plan staff training as needed.
- Technical support is provided by AVA. support.ava@stockport.gov.uk (0161)4742240. Requests for technical support may be made by all members of staff through Google Sheets AVA Job Reporter
- Class teachers are responsible for ensuring that children have opportunities for learning IT skills and importantly for using IT across the curriculum.
- Pupils may use IT independently, in pairs, with a TA or in a group with a teacher.

Staff Training

At Norris Bank we have a high expectation on teachers to use IT, for example through use of the Google Workspace for Education. All classrooms are equipped with an interactive panel linked to a PC which is running Windows 10 Professional.

The IT coordination team will periodically provide an audit of staff training needs as part of the action plan. This has included a visit by a PurpleMash trainer and the introduction of a new progression and assessment framework. Members of the IT team attend network opportunities provided by Stockport LEA and Computing At Schools through the Stockport Primary Hub

Administrative Systems

The school administration (SIMS) is separate from the CC3 network with access available through the school office. The school's onsite curriculum server continues to host staff, shared and media folders, although the school is looking into the possibility of a future cloud based solution. Teaching staff have 24/7 access to the curriculum server drives through a webclient service hosted by SSELN.

Out of Hours Use and Extra-Curricular Opportunities

- Currently the ICT suite is used by the after-school care club, 'Branching Out' informally between 3:20 and 5:45 p.m. From 8:30 the IT suite is used by children following a dyslexia intervention programme.
- We run a 'Digital Leaders' scheme for children in Years 3 and 4. Digital Leaders have the opportunity to support younger children, for example in Year R with their computing and to develop their own skills on Friday lunchtimes. Children are invited to apply for the position of digital leader on two occasions during the year.
- Within our parent community we have IT professionals who have offered to run coding clubs for groups of KS2 children. These have proven to be oversubscribed and highly successful, often making use of resources such as micro:bits or Scratch.

Health and Safety

- Access to the internet is filtered by Stockport LEA's chosen digital safety partner, Smoothwall (See Acceptable Use Policy below).
- No food and drink is to be taken into the computer suite by adults or children.
- Faults with equipment are to be reported using Google Sheets AVA Job Reporter.

Security

All IT equipment is security marked and noted in the school inventory. This inventory includes the serial number of each item.
All portable electronic devices, i.e. iPads and Chrome devices are to be returned to secure storage (charging trolleys) at the end of each day or when the classroom is unoccupied for an extended period. Chrome device trolleys are stored in the IT suite overnight and charged.
AVA will be responsible for regularly updating antivirus software.
Digital security is managed by Stockport LEA's chosen digital safety partner, Smoothwall (See Acceptable Use Policy below).

Norris Bank E-Safety and Acceptable Internet Use Policy

Rationale

The purpose of this policy is to:

1. Set out the principles expected of all members of the community at Norris Bank Primary School with respect to the use of IT-based technologies.
2. Safeguard and protect the children and staff of Norris Bank Primary School.
3. Have clear structures to deal with online abuse including peer on peer within our community.
4. Ensure that all members of the community are aware that unlawful or unsafe behaviour is unacceptable and what the consequences of inappropriate use can be.
5. Make all members of staff aware of the monitoring and filtering systems that are in place to keep children digitally safer and of their roles and responsibilities in these two areas.

The main areas of risk are as follows:

Children's physical and mental health can be affected by:

1. **Content**

The risk of children being exposed to indecent or age-inappropriate content.

2. **Contact**
Children being inappropriately contacted (groomed), subjected to online bullying or abuse or having their identity or passwords stolen.
3. **Conduct**
The disclosure of personal information, the amount of time spent online and inappropriate behaviour online towards others.

This policy applies to all members of The Norris Bank School community (including staff, governors, children, visitors (e.g. student teachers), volunteers (e.g. reading volunteers) and parents/carers, visitors who have access to and are users of the school's computing systems, both in and out of school.

The Education and Inspections Act empowers the head teacher to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and responsibilities

Head teacher / Designated Safety Lead (DSL)

- To take overall responsibility for online safety provision.
- To take overall responsibility for data and data security.
- To ensure the school uses an approved, filtered internet service, which complies with current statutory requirements, currently 'SmoothWall', Stockport's internet filter.
- To oversee and, when appropriate, act upon a weekly filtering and monitoring report and resultant safeguarding concerns.
- To be responsible for ensuring that staff receive suitable training to carry out their online safety roles including filtering and monitoring.
- To promote an awareness and commitment to online safeguarding throughout the school community.
- To communicate regularly with SLT and the designated online safety governor to discuss current issues.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident and to complete an online safety log in the event of an incident.
- To liaise with the LEA and is updated in e-safety issues and legislation.
- To oversee the delivery of the online safety element of the computing curriculum and ensure that this is embedded across the curriculum.

Safeguarding Governor

- To ensure that the school follows all current online safety advice to keep the children and staff safe.
- To approve the online safety policy and review the effectiveness of the policy. This will be carried out by the curriculum sub-committee receiving regular information about online safety incidents and monitoring reports.
- To support the school in encouraging parents and the wider community to become engaged in e-safety activities

IT Service Provider (Stockport / Smoothwall)

- To ensure that users may only access the school's network through an authorised and properly enforced password protection policy, in which passwords are regularly changed.
- To provide and maintain filtering and monitoring systems which ensure the detection of misuse and malicious attack.
- To provide a regular filtering and monitoring report to the DSL / Headteacher.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure appropriate backup procedures of the curriculum and admin servers exist so that critical information and systems can be recovered in the event of a disaster.
- Ensure devices are protected with a firewall, access to which is protected by multi-factor authentication and a specified IP-allow list.

Teachers

- To embed online safety issues in all aspects of the curriculum and other school activities.
- To supervise and guide children carefully when engaged in learning activities involving online technology (including, extra-curricular activities if relevant).
- To ensure that when using research skills, children are becoming aware of legal issues relating to electronic content such as copyright laws.
- For all school related activities and communication related to their employment at the school to make use of their 'school' Gmail account i.e. firstname.surname@norrisbank.stockport.sch.uk
- To NOT share their password with anyone in rider that they can access their school device.
- The computing curriculum team takes day to day responsibility for online safety issues and, together with the Personal Social Health and Relationship lead has a role in establishing and reviewing the school online safety policy.

All staff

- To read, understand and help promote the school's e-safety policy.
- To read, understand, sign and adhere to the school's Staff Handbook.
- To be aware of online safety issues related to the use of mobile phones and other devices and how their use is monitored through the school's filtering and monitoring system.
- To report any suspected misuse or problem to the DSL / Headteacher.
- To model safe, responsible and professional behaviour in their own use of technology.
- To ensure that any digital communications with children should be on a professional level and only through school based systems, never through personal mechanisms, i.e. email, text, mobile phone or social networking.
- For all school related activities and communication related to their employment at the school to make use of their 'school' Gmail account i.e. firstname.surname@norrisbank.stockport.sch.uk
- To NOT share their password with anyone in rider that they can access their school device.

Children

- Read, understand, sign and adhere to the acceptable use agreement.
- To begin to have an understanding of research skills and copyright regulations.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials.
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand school policy on the use of mobile phones and other devices.

- To know and understand school policy on the taking and use of images and on cyber-bullying.
- To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.

Parents and carers

- To support the school in promoting online safety and endorse the Parents' acceptable use agreement which includes the children' use of the Internet and the school's use of photographic and video images.
- To access the school website and their child/children's Gmail accounts in accordance with the relevant school acceptable use agreement.
- To consult with the school if they have any concerns about their children's use of technology.
- To contact teachers and other members of school staff through authority regulated e-mail channels i.e. firstname.surname@norrisbank.stockport.sch.uk

External groups

Any external individual or organisation will sign an acceptable use agreement prior to using any equipment or the Internet within school or making use of the wireless internet.

Communication

The policy will be communicated in the following ways:

1. Posted on the school website.
2. Be part of the school induction pack for new staff and visiting student teachers.
3. Acceptable use agreements discussed with children at the start of each key stage.
4. Acceptable use agreements to be issued to whole school community, usually on entry to the school.
5. Acceptable use agreements to be held on pupil and personnel files.

Handling complaints

Members of the SLT act as a first point of contact for any complaint. Any complaint about staff misuse is referred to the head teacher. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LEA child protection procedures.

Review and Monitoring

The online E-safety policy is referenced from within other school policies (computing, child protection, anti-bullying, behaviour, PSHRE). The online E-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school. The online E-safety policy has been written by the computing curriculum team and is current and appropriate for its intended audience and purpose. There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors.

Education and Curriculum

Pupil online safety curriculum

Norris Bank Primary School has an online E-safety education programme as part of the computing and PSHRE curriculum. This is reflected in the Acceptable Use Agreement (see below) as well as curriculum overviews for each year e.g. PurpleMash Units of work.

Incident Management

In our school:

1. Online activity is monitored through 'Smoothwall' and incidents of concern are sent to the DSL in a report.
2. All members of the school community are encouraged to be vigilant in reporting issues knowing that issues will be dealt with quickly and sensitively.
3. Support is actively sought from other agencies (e.g. LEA) as needed in dealing with online safety issues.
4. Reviews of online safety incidents take place. This contributes to developments in policy and practice in e-safety within the school.
5. Parents and carers are specifically informed of online safety incidents involving young people for whom they are responsible.
6. We will contact the police if one of our staff or children receives online communication that we consider is particularly disturbing or breaks the law.

Managing the IT and computing infrastructure, Internet access, security (virus protection) and filtering

Our school:

- Uses 'Smoothwall' as a filtering and monitoring service.
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
- Only unblocks other external social networking sites for specific purposes e.g. internet literacy lessons.
- Blocks pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level e.g. YouTube.
- Works in partnership with SSELN to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- Ensures staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures children only publish within an appropriately secure environment: Google Classroom or PurpleMash.
- Requires staff to preview websites before use and encourages use of the 'Explore' element of Google Classroom as a key way to direct children to age appropriate web sites;
- Informs all users that internet use is monitored.
- Understand what sanctions result from misuse – through staff meetings and teaching programme;
- Refers any material we suspect is illegal to the appropriate authorities – Police – and the LEA.

Network management (user access, backup)

Our school:

1. Uses individual, audited log-ins for all users through the school's AVA administered RM system (staff only) or Google Classroom (staff and children).

2. Ensures that storage of all data within the school will conform to the UK data protection requirements.

3. Ensures staff read and sign that they have understood the school's online E-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to the service is through a unique, audited username and password.

4. Controls staff access to the SIMS through a separate password for data security purposes.

5. Provides children with an individual network log-in username.

6. Makes clear that no one should log on as another user and makes clear that children should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
7. Has set-up the network with a shared work area for staff.
8. Requires all users to always log off when they have finished working or are leaving the computer unattended.
9. Asks that when a user finds a logged-on machine, they always log-off and then log-on again as themselves.
10. Has set-up the network so that users cannot download executable files / programmes.
11. Scans all mobile equipment with anti-virus / spyware before it is connected to the network.
12. Maintains equipment to ensure health and safety is followed and that equipment is installed and checked by approved suppliers and LEA electrical engineers.
13. Has separate curriculum and administration networks. Access to SIMS is set-up so as to ensure staff users can only access modules related to their role; e.g. teacher's access report writing folders.
14. Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems.
15. Provides children and staff with access to content and resources through Google Classroom which staff and children access using their username and password.
16. Reviews the school IT systems regularly with regard to health and safety and security.

Password policy

Our school:

Makes it clear that staff and children must always keep their password private, must not share it with others and must not leave it where others can find it.

E-mail

Our school:

1. Provides staff and children with a Gmail account for their use and makes clear personal email should be through a separate account.
2. Does not publish personal email addresses of children or staff on the school website.
3. Will contact the police if one of our staff or children receives an email that we consider is particularly disturbing or breaks the law.
4. Will ensure that email accounts are maintained and up to date.
5. Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
6. Asks children to sign the school Acceptable Use Agreement to say they have read and understood the e-safety rules, including e-mail.

Staff

1. Only use their school Gmail account for professional purposes.
2. Understand that access in school to external personal email accounts may be blocked.
3. Know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper.
4. ClassDojo is only used for general announcements and class news; all other correspondence is made through the school email channel.

School website

1. The headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

2. Uploading of information is restricted to our website authorisers e.g. school administrator or computing lead. The school website complies with the statutory DfE guidelines for publications.
3. Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
4. The point of contact on the website is the school address, telephone number and email contact address. Home information or individual email identities will not be published;
5. Photographs published on the web do not have full names attached.
6. We do not use children's names when saving images in the file names or in the tags when publishing to the school website.

Extremism and Anti-terrorism

There is no place for the expression of extremist views of any kind in our school. As a school we recognise that extremism and exposure to extremist materials and influences can lead to poor outcomes for our students. We also recognise that if we fail to challenge extremist views we are failing to protect our students. Extremists aim to develop destructive relationships between different communities by promoting division, fear and mistrust of others based on ignorance or prejudice and thereby limiting the life chances of young people. Education is a powerful weapon against this; equipping young people with the knowledge, skills and critical thinking, to challenge and debate in an informed way. Therefore we will provide a broad and balanced curriculum, delivered by skilled professionals, so that our pupils are enriched, understand and become tolerant of difference and diversity and also to ensure that they thrive, feel valued and not marginalised.

Social networking

1. Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications. The school makes use of Classdojo as a reward system but also to message parents and share news about learning with the parents and carers of the children of their class. Classdojo's privacy statement can be found at https://www.classdojo.com/en-gb/privacycenter/?redirect=true

2. School staff will ensure that in private use:
   a) No reference should be made in social media of the school, to the children, parents or carers or school staff.
   b) They do not engage in online discussion on personal matters relating to members of the school community past or present.
   c) Personal opinions should not be attributed to the school or local authority.
   d) Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Equipment and Digital Content

Personal mobile phones and mobile devices

All staff need to refer to the Mobile Phone Policy in the Staff Handbook:

1. Mobile phones that are brought into school are entirely at the staff member's, children's, parents' or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
2. Children do not bring mobile phones into school but we understand that for older juniors they may form part of a child's before and after-school arrangements. These telephones are turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.

3. Staff members may use their phones during school break times (in designated adult only non-teaching areas e.g. staffroom or off site).
4. All visitors are requested to keep their phones on silent.
5. The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided.
6. The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time. These devices are also subject to filtering and monitoring by Smoothwall when connected to the school's WiFi network.
7. Where parents, students or staff need to contact each other during the school day, they should do so only through the office.
8. Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times and out of sight.
9. Seizure of devices from children by the police might be necessary to progress inquiries and inform safeguarding decisions although this would only occur following referral through Multi-Agency Safeguarding Hub (MASH).

Digital images and video

In our school:

1. We gain parental or carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.
2. We do not identify children in online photographic materials or include the full names of children in the credits of any published school produced video materials.
3. If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.
4. The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose e.g. Classdojo.
5. Children are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work.
6. School acknowledges the growing prevalence of the sharing of nude images and non-consensual sharing and online sexual abuse. This may also include the use of AI generated images and sharing with adults that pose as a child to sexually abuse or financial blackmail. Although this form of exploitation is mostly prevalent with older (i.e. secondary age) children, the access that many of our KS2 children have to mobile phones does not preclude it occurring within our school community.

Asset disposal

- Details of all school-owned hardware is recorded on a cloud based system overseen by AVA.
- All redundant equipment will be disposed of through an authorised agency (AVA) This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

Norris Bank Primary School Internet Use Agreement

I want to use our computers and the internet. I know that there are certain rules about what I should do online. I agree to follow these rules and my parents agree to help me follow these rules:

1. I will not give my name, address, telephone number, school, or my parents' names, address, or telephone number; to anyone I meet on the computer.

2. I understand that some people online pretend to be someone else. Sometimes they pretend to be kids, when they're really adults. I will tell my parents about people I meet online. I will also tell my parents before I answer any e-mails I get from or send e-mails to new people I meet online.

3. I will not fill out any form online that asks me for any information about myself or my family without asking my parents first.

4. I will not buy or order anything online without asking my parents or give out any credit card information.

5. I will not get into arguments or fights online. If someone tries to start an argument or fight with me, I won't answer him or her and will tell my parents.

6. If I see something I do not like or that I know my parents don't want me to see, I will click on the back button or log off.

7. If I see people doing things or saying things to other kids online I know they're not supposed to do or say, I'll tell my parents.

8. I won't keep online secrets from my parents.

9. If someone sends me any pictures or any e-mails using bad language, I will tell my parents.

10. If someone asks me to do something I am not supposed to do, I will tell my parents.

11. I will not call anyone I met online, in person, unless my parents give permission.

12. I will never meet in person anyone I met online, unless my parents give permission.

13. I will never send anything to anyone I met online, unless my parents give permission.

14. If anyone I met online sends me anything, I will tell my parents.

15. I will not use something I found online and pretend it's mine.

16. I won't say bad things about people online, and I will practise good etiquette.

17. I won't use bad language online.

18. I know that my parents want to make sure I'm safe online, and I will listen to them when they ask me not to do something.

19. I will help teach my parents more about computers and the Internet.

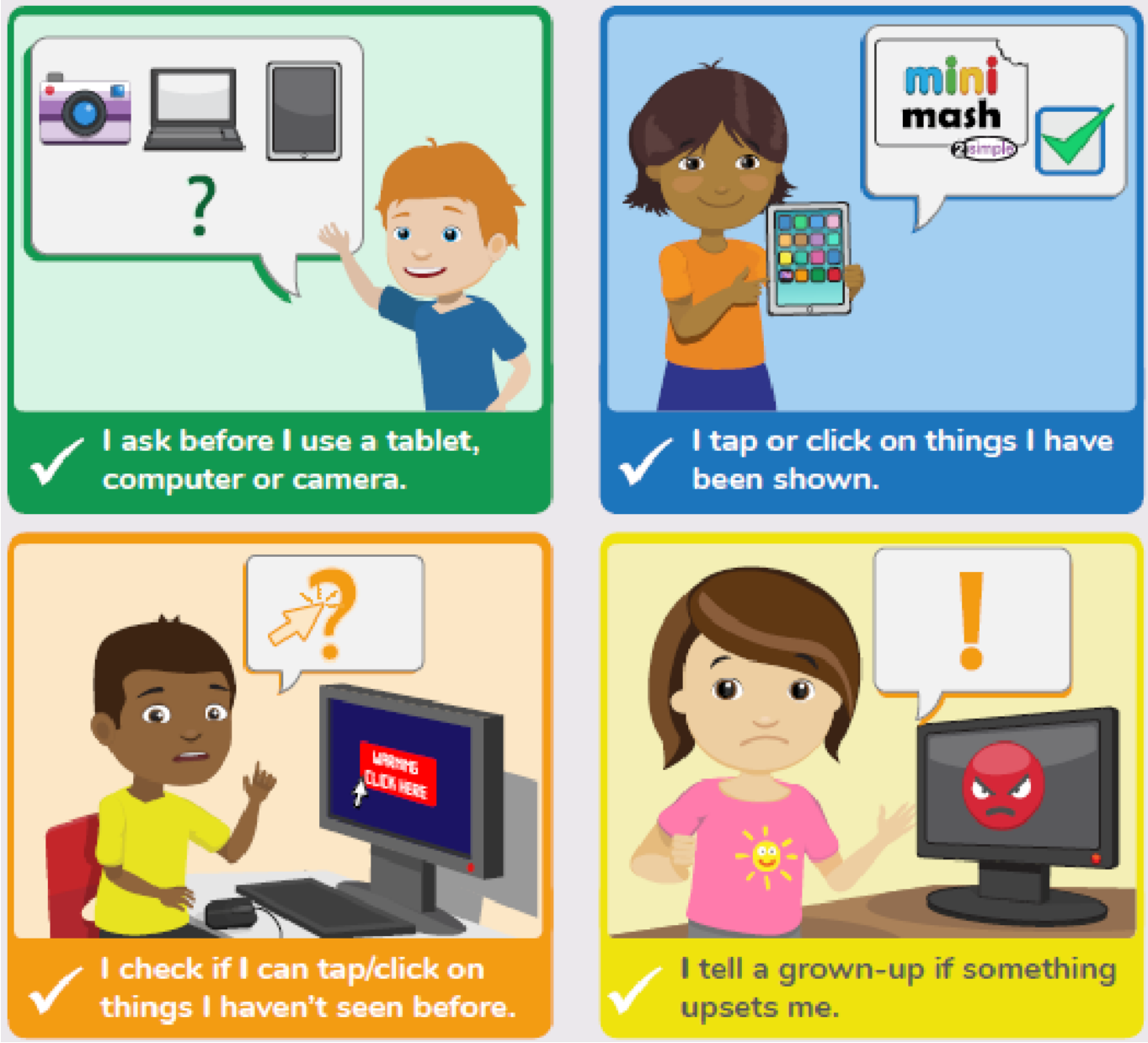
20. I will practise safe computing, and check for viruses whenever I borrow a USB from someone or download something from the Internet.

_____
I promise to follow these rules.
(Child's Signature)

_____
I promise to help my child follow these rules.
(Parents Signature)

Norris Bank Primary School.

Acceptable Use Agreement – Reception



Child's name	Class
Teachers name	
Teachers signature	
Date	

Norris Bank Primary School.

Acceptable Use Agreement – Key Stage 1

- ✓ I always ask an adult if I want to use a computer.
- ✓ I take care of the computer and other equipment.
- ✓ I only open activities that an adult has told me or allowed me to use.
- ✓ I tell an adult if I see something that upsets me on screen.
- ✓ I ask an adult for help if I am not sure what to do or if I think I have done something wrong.
- ✓ I keep my password safe and don't use anyone else's.
- ✓ I know I must not share personal information like my address or birthday online.
- ✓ I know I must not communicate with strangers online.
- ✓ I am always polite when communicating or working with others on the computer.

I understand these rules and know that if I don't follow them I might not be allowed to use a computer.

Child's name	Class
Teachers name	
Teachers signature	
Date	

Norris Bank Primary School.

Acceptable Use Agreement – Key Stage 2

I understand that I must use school computing equipment in a responsible way, to keep myself, other children and the computer systems safe.

- ✓ I only use computing equipment with an adult's permission.
- ✓ I know that school checks my files and the online sites I visit, and will contact my parents/ carers if they are concerned about me.
- ✓ I don't use school equipment for personal use unless I have permission from an adult.
- ✓ I don't share my username and password and don't use anyone else's.
- ✓ I know what personal information is (like my name, address, school name, phone number) and will not share my own or someone else's online.
- ✓ I tell an adult if I see something that makes me feel uncomfortable, sad, afraid or angry on a computer or other device.
- ✓ I will not deliberately look for, save or send anything that could make others upset.
- ✓ I respect computing equipment and will tell an adult if I notice that something isn't working or is damaged.
- ✓ Before I share, post or reply to anything online I will T.H.I.N.K.

- ✓ I am responsible for my actions, in and out of school
- ✓ I understand that if I behave negatively whilst using technology towards other members of my school (e.g. cyber-bullying, sharing other people's information or photographs) that school will inform my parents/ carers and take appropriate action.

Child's name	Class
Teachers name	
Teachers signature	
Date	