E-safety (Online) Policy

Kennel Lane School

Approved by:	Senior Leadership Team	**Date:**	Autumn Term 2023
Last reviewed on:	Autumn Term 2022		
Next review due by:	Autumn Term 2026		

Contents

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on learners' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Board will co-ordinate regular meetings with appropriate colleagues to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All Governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3)

3.2 The Headteacher

The Headteacher is responsible for ensuring that colleagues understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead
Details of the school's DSL and deputies are set out in our Safeguarding and Child Protection Policy.

The DSL takes lead responsibility for e-safety/online safety in school, in particular:
- Supporting the Headteacher in ensuring that colleagues understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT service provider and other colleagues, as necessary, to address any e-safety/online safety issues or incidents
- Ensuring that any e-safety/online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's Regulation and Co-Regulation Policy
- Updating and delivering colleague training on e-safety/online safety (Appendix 4 contains a self-audit for colleagues on e-safety/online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or Governing Body

This list is not intended to be exhaustive.

3.4 The ICT service provider
The ICT service provider is responsible for:
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep learners safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All colleagues and volunteers
All colleagues, including contractors, agency colleagues, and volunteers are responsible for:
- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3), and ensuring that learners follow the school's terms on acceptable use (Appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's Regulation and Co-Regulation Policy

This list is not intended to be exhaustive.

3.6 Carers and Parents
Carers and parents are expected to:
- Notify a member of the school team or the Headteacher of any concerns or queries regarding this policy
- Understand their young person has had access to the terms on acceptable use of the school's ICT systems and internet, at a level that is appropriate for them (Appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 3).

4. Educating learners about e-safety/online safety
Learners will be taught about online safety as part of the curriculum:

From September 2020 schools have to teach:
- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Learners in **Key Stage 1**, where appropriate, will be taught to:
- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Learners in **Key Stage 2**, where appropriate, in addition to the above, will be taught to:
- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

Learners in **Key Stage 3**, where appropriate, in addition to the above, will be taught to:
- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Learners in **Key Stage 4 and 5**, where appropriate, in addition to the above, will be taught to:
- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of their education**, where appropriate, it is hoped learners will know and/or have an understanding at a level appropriate to them of some or all of the following:
- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise learners' awareness of the dangers that can be encountered online and may also invite speakers to talk to learners about this.

5. Educating carers and parents about online safety

The school will raise carers and parents' awareness of internet safety in letters, newsletters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during carer and parents' information events.

If carers and parents have any queries or concerns in relation to e-safety/online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of the school team or the Headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Regulation and Co-Regulation Policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that, where appropriate, learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Where appropriate, the school will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and tutors will discuss cyber-bullying with their groups, and the issue will be addressed in assemblies.

Teaching colleagues are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Relationship, Sex and Health Education (RSHE), and other subjects where appropriate.

All colleagues, Governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners, as part of safeguarding training.

The school also sends information/leaflets to carers and parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's Regulation and Co-Regulation Policy. Where illegal, inappropriate or harmful material has been spread among learners, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School colleagues have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on learners' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, school colleagues must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching and learning, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the school colleague in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of learners will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on learners' electronic devices will be dealt with through the school's Complaints Policy.

7. Acceptable use of the internet in school
All learners, colleagues, volunteers (where appropriate) and Governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by learners, colleagues, volunteers, Governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the Acceptable Use Agreements in Appendices 1, 2 and 3.

8. Learners using mobile devices in school
Learners may bring mobile devices into school, but must be handed to their class teacher/tutor in the morning during registration to re-affirm no learners are permitted to use them during:

- Lessons
- Tutor group time
- Break or lunch times
- Or any other activities organised by the school

More details can be found in our Mobile Phone Policy.

9. Colleagues using work devices outside school
Colleagues using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 3.

Colleagues must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If colleagues have any concerns over the security of their device, they must seek advice from our ICT service provider.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse
Where a learner misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a colleague misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with colleague disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training
All new colleagues will receive training, as part of their induction, on safe internet use and e-safety/online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All colleagues will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

12. Monitoring arrangements

Behaviour and safeguarding issues related to online safety; Behaviour incidents are recorded on Sleuth and Safeguarding incidents are recorded on CPOMS.

This policy will be reviewed every 3 years by the school's Computing Leads. At every review, the policy will be shared with the Governing Body.

13. Links with other policies

This online safety policy is linked to our:

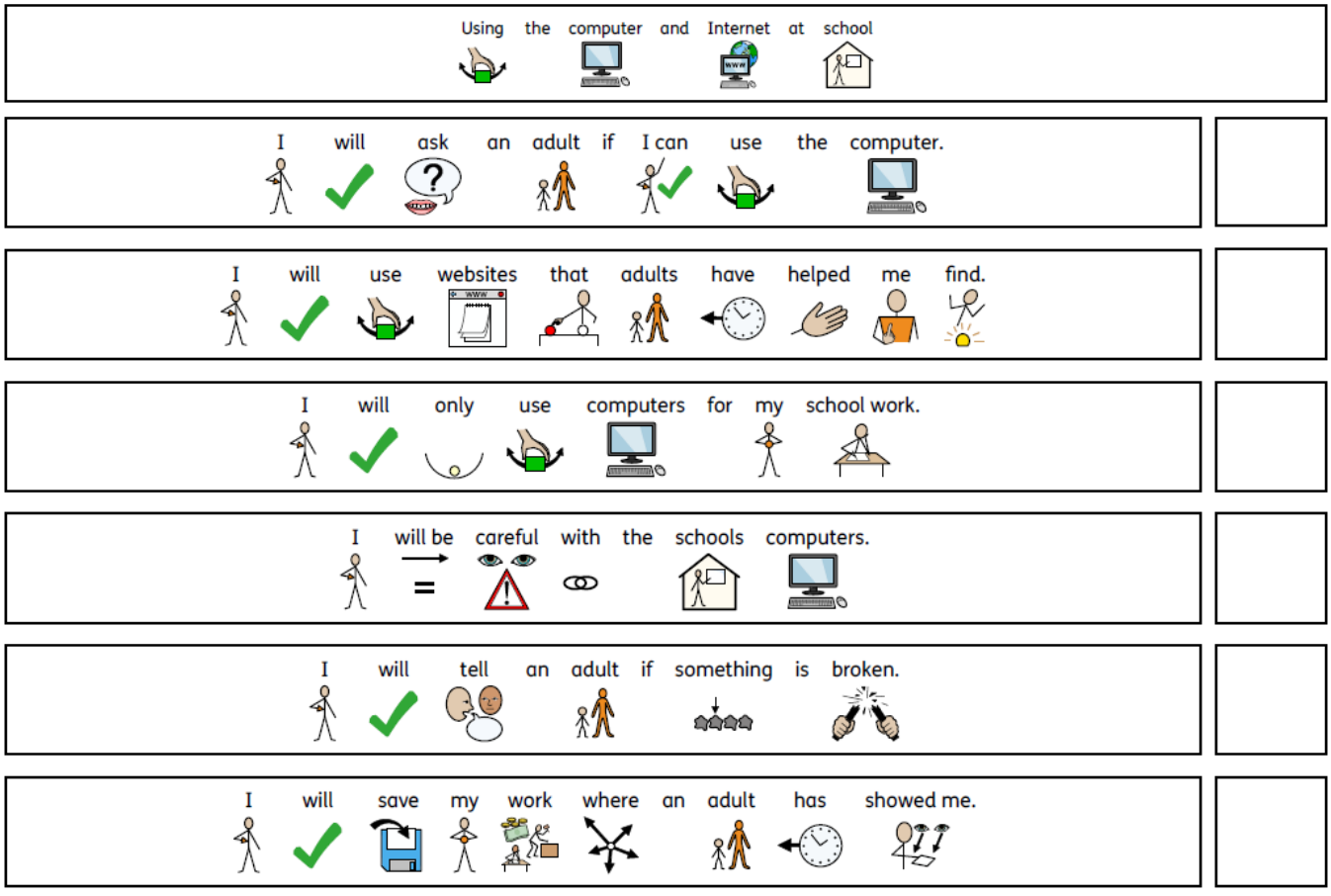
- Safeguarding and Child Protection Policy
- Regulation and Co-Regulation Policy
- Code of Conduct
- Data protection policy and privacy notices
- Complaints Policy
- Mobile Phone Policy
- Acceptable Use Policy

Appendix 1: EYFS and KS1 Acceptable Use Agreement

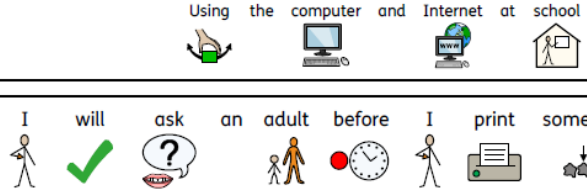
ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS	
Name of learner:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• I will be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (learner):	**Date:**

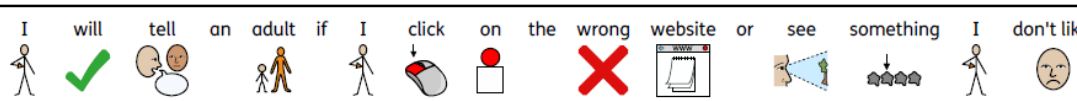


Using the computer and Internet at school

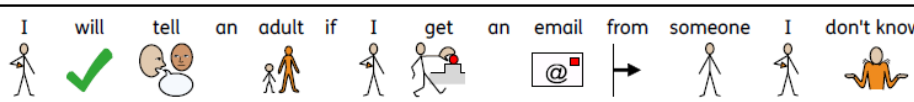


I will ask an adult before I print something.

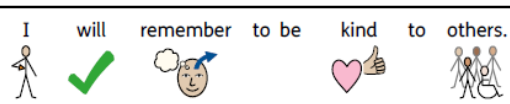
I will tell an adult if I click on the wrong website or see something I don't like.



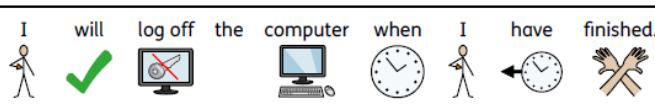
I will tell an adult if I get an email from someone I don't know.



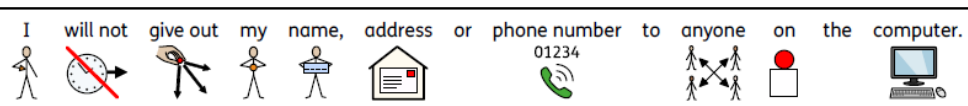
I will remember to be kind to others.



I will log off the computer when I have finished.

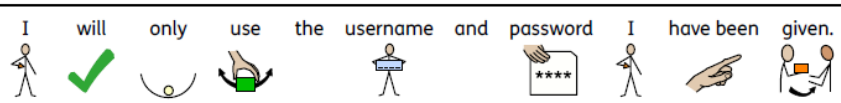


I will not give out my name, address or phone number to anyone on the computer.



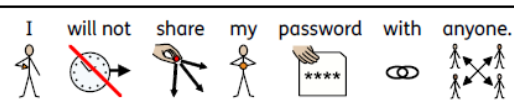
Using the computer and Internet at school

I will only use the username and password I have been given.



I will try to remember my username and password.

I will not share my password with anyone.



Sign name

Date

Appendix 2: KS2-KS5 Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS	
Name of learner:	

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

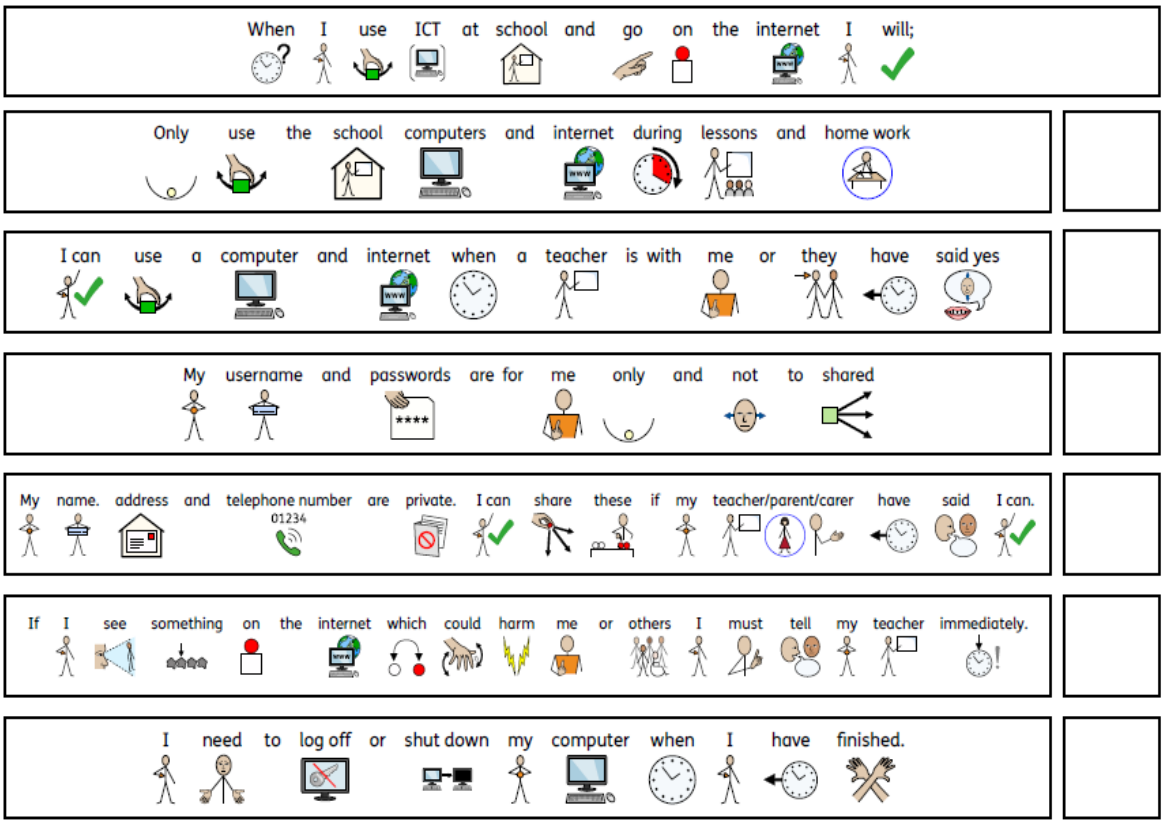
- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (learner):	**Date:**



When I use ICT at school and go on the internet I will not;

Not go on websites for social media, chat rooms, or gaming sites unless my teacher has said I can

Not open attachments or follow links in emails without asking my teacher first

Not use unsafe language when talking to someone online or writing an email

Not Log on to a school computer using another persons name or password

Not arrange to meet someone without telling or having an adult with me

If I bring in a phone, electronice device into school;

If I bring my phone into school I need to give to my teacher

If I bring in an electronice device I need to give to my teacher

At the end of the school day my teacher will give me back my phone/ electronice device

Sign name:

Date:

Appendix 3: Colleagues, Governors, volunteers and visitors Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR COLLEAGUES, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of colleague/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of learners without checking with teachers first • Share confidential information about the school, its learners or colleagues, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a learner informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that learners in my care do so too.	
Signed (colleague/Governor/volunteer/visitor):	**Date:**

Appendix 4: E-safety/Online safety training needs – Self audit for colleagues

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of colleague/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a learner approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for colleagues, volunteers, Governors and visitors?	
Are you familiar with the school's acceptable use agreement for learners?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: E-safety/Online safety incident reporting

CPOMS

Back

Student: Begin typing a student's name

Incident:

Categories: Attendance | Cause for Concern | Contact with External Agency | Family Support Intervention | Medical | Monitoring | Parental Contact | Safeguarding meetings | Strategy Meeting

Linked student(s): Begin typing a student's name

Type a student's name to link them to this incident.

Maps

Date/Time: 15/09/2023 22:18

Status: Active

Assign to: Begin typing a staff member's name

Files: Click to browse or drag a file to upload

Alert Staff Members: Begin typing a staff member's name

Type a colleague's name or select an alert group to alert them to this incident. Colleagues highlighted in red would not normally be able to view this incident.

Agency Involved

Add to planner

Submit Incident