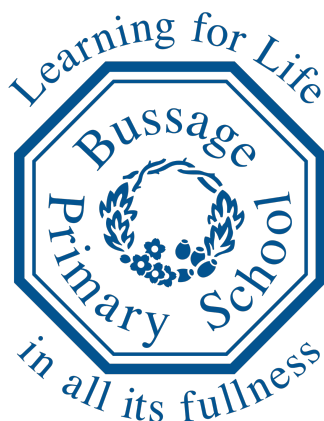


Policy on Online Safety



Next review: Spring 2025

Bussage Primary School is a Church of England Voluntary Aided Primary School and this policy is written within the context of the Christian faith, practice and values which underpin our ethos, and which are in keeping with our Trust Deed.

Our school's Christian ethos is that all pupils, whatever their ability or talents, are created in the image of God, and are loved equally by him.

Our school's mission is to provide a learning and development environment in which all pupils and staff can make the most of their God given potential and aspire to "be the best that they can be."

Our school vision is built upon the four cornerstones of WISDOM, HOPE, COMMUNITY and DIGNITY.

For children to be able to learn effectively and to live life to it fullness they must be safe and secure and they must feel safe and secure. In our school, Child Protection and Safeguarding is always our top priority.

Statutory	Yes (as part of SG)
Web-Site	Yes
Owner	Headteacher
Principle Author(s)	Headteacher
Committee	Comms

Delegation and Review	
Max. Permitted	Governing Body
Determined	Governing Body
Review	Governors Decide
Frequency	2 Years

Contents

1. Aims	2
2. Legislation and guidance	2
3. Roles and responsibilities	2
4. Educating pupils about online safety	4
5. Educating parents about online safety	5
6. Cyber-bullying	5
7. Acceptable use of the internet in school	6
8. Staff using work devices outside school	6
9. How the school will respond to issues of misuse	7
10. Training	7
11. Monitoring arrangements	7
12. Links with other policies	7
Appendix 1: Acceptable use agreement (pupils and parents/carers)	8
Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)	11
Appendix 3: Online safety training needs – self-audit for staff	13
Appendix 4: Online safety incident report log	14

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, 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 statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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 pupils’ 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.

Policy on Online Safety

The governing body will co-ordinate regular meetings with appropriate staff 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 2)

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) [and deputy/deputies] are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on 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 board

This list is not intended to be exhaustive.

3.4 The ICT manager (Thomas Keble)

The ICT manager (Thomas Keble) is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) 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 behaviour policy

Policy on Online Safety

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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 behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <https://www.childnet.com/ufiles/Parents-and-carers-resource-sheet-1019.pdf>

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 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the Purple Mash computing curriculum. Every year, each class will complete a dedicated online safety unit as part of their computing lessons. Additional online safety objectives are integrated, where appropriate, throughout the other Purple Mash units taught across the year and through a selection of SCARF PSHE lessons. The safe use of social media and the internet will also be covered in other subjects where relevant.

In **Key Stage 1**, pupils 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

Policy on Online Safety

Pupils in **Key Stage 2** 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

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 pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. They will promote the importance of online safety by taking part in Safer Internet Day each year.

5. Educating parents about online safety

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

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher.

Concerns or queries about this policy can be raised with any member of staff 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 Anti-bullying Policy.)

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Anti-bullying Policy. Where illegal, inappropriate or harmful material has been spread among pupils, 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 staff 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 pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

Policy on Online Safety

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

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

If inappropriate material is found on the device, it is up to the staff member 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 pupils 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 pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Refer to Appendices 1 and 2 which include all versions of the acceptable use policy.

There are three different acceptable use agreements completed during the first term by pupils to ensure the language used is appropriate for them.

1. EYFS Acceptable use policy – completed by Rainbows
2. KS1/LKS2 Acceptable use policy – completed by Year 1 and Year 3
3. KS2 Acceptable use policy – completed by Year 5

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 pupils, staff, 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 and 2.

8. Staff using work devices outside school

Staff members 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 2.

Staff 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 staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

9. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member 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 the staff 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.

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members 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, e-bulletins and staff meetings).

The DSL and deputy (DDSL) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years.

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 child protection and safeguarding policy.

11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed every two years by the DSL. At every review, the policy will be shared with the governing board.

Any incidents will be reported within the Head teacher report to the Full Governing Body.

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Acceptable use agreement (pupils and parents/carers)

**Bussage C of E (Aided) Primary School
Pupil Acceptable Use Policy: EYFS - Rainbows**

See separate accompanying document.

Online Safety Policy_Acceptable Use Agreement EYFS 2023.pdf

which can be completed by the EYFS lead with the Children and counter-signed electronically by the parent/carer.

Bussage C of E (Aided) Primary School
Pupil Acceptable Use Policy: KS1 / LKS2

I choose to stay safe

- I know what my personal information is and I will not share it online. ☐
- I will tell an adult straight away if I see anything scary or anything that makes me feel uncomfortable online and I will not show it to other children. ☐
- If anyone online asks me to meet them in real life, I will tell an adult such as my teachers or parents straight away. ☐
- I will never arrange to meet anyone in person after I have met them online. ☐

I choose to be kind and helpful

- I will only use polite language when using the computers and I will not write anything that might upset someone or give the school a bad name. ☐

I choose to be honest

- I will never use other people's usernames and passwords on computers left logged in by them. ☐
- I will only use the school's computer systems for things a teacher has given me permission to do. ☐
- I will not copy, remove or change any other person's files, without their knowledge and permission.

I choose to look after property

- I will be careful with computing equipment. ☐
- I will tell an adult straight away if I notice computing equipment is damaged. ☐

I understand that:

- I know that pictures on the internet can belong to the person who put them there. ☐
- I know that some things on the internet are not true. ☐
- For my own and others' safety and the safety of the school's computer systems, the school will monitor my use of the computer systems, email and other digital communications. ☐
- The school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information). ☐
- If I choose not to keep to this agreement, I may not be allowed to use computers, laptops, LearnPads or other equipment until the school feels it is safe and right for me to do so. ☐

Child's Name

Signed

Date

I understand that my child has agreed to the above policy and support the school in keeping my child safe online.

Parent's Signature

Date

Bussage C of E (Aided) Primary School

Pupil Acceptable Use Policy

I choose to stay safe

- I will not disclose or share personal information about myself or others when online. ☐
- If I find something that I think I should not be able to see, I will turn off the screen or close the lid on a laptop or cover on a LearnPad. I will tell an adult straight away and **not show it to other children**. ☐
- I will tell an adult straight away if I see any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable online and **not show it to other children**. ☐
- I will not access or share any materials which are inappropriate or may cause harm or distress to others. If I accidentally do so, I will tell an adult straight away and **not show it to other children**. ☐
- If anyone online asks me to meet them in real life, I will tell an adult such as my teachers or parents straight away. ☐
- I will never arrange to meet anyone in person after I have met them online. ☐

I choose to be kind and helpful

- I will only use polite language when using the computers and I will not write anything that might upset someone or give the school a bad name. ☐

I choose to be honest

- I will never use other people's usernames and passwords on computers left logged in by them. ☐
- I will only use the school's ICT systems for things a teacher has given me permission to do. ☐
- I will not download anything without permission. ☐
- I will not bring my own devices (mobile phones / USB devices etc) to school unless I have been given special permission by my teacher. ☐
- I will respect others' work and property and will not access, copy, remove or change any other user's files, without their knowledge and permission. ☐

I choose to look after property

- I will immediately report any damage or faults involving equipment or software, however this may have happened. ☐
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes. ☐
- I will not install or attempt to install programmes, or store programmes on a school computer, nor will I try to alter computer settings. ☐
- I will not attempt to use the school's ICT systems for file-sharing. ☐

I understand that:

- I will acknowledge sources of information and images copied from the internet using a reference. ☐
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may be incorrect and may even be a deliberate attempt to mislead me. ☐
- For my own and others' safety and the safety of the school's ICT systems, the school will monitor my use of the ICT systems, email and other digital communications. ☐
- The school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information). ☐
- If I choose not to keep to this agreement I may not be allowed to use computers, laptops or other equipment until the school feels it is safe and right for me to do so. ☐

Child's Name

Signed

Date

I understand that my child has agreed to the above policy and support the school in keeping my child safe online.

Parent's Signature

Date

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications. ☐
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, website etc) out of school. ☐
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. ☐
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person. ☐

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission. ☐
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. ☐
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured. ☐
- I will not use chat and social networking sites in school. ☐
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. ☐
- I will not engage in any on-line activity that may compromise my professional responsibilities. ☐

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. ☐
- I will not use personal email addresses on the school ICT systems. ☐
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes. ☐
- I will ensure that my data is regularly backed up. ☐
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. ☐
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work. ☐
- I will not disable or cause any damage to school equipment, or the equipment belonging to others. ☐
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy Where personal data is transferred outside the secure school network, it must be encrypted. ☐
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority. ☐
- I will immediately report any damage or faults involving equipment or software, however this may have happened. ☐

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work ☐
- Where work is protected by copyright, I will not download or distribute copies (including music and videos). ☐
- I understand that I am responsible for my actions in and out of school: ☐
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school. ☐
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police. ☐

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications. ☐
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, website etc) out of school. ☐
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. ☐
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person. ☐

Policy on Online Safety

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission. ☐
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. ☐
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured. ☐
- I will not use chat and social networking sites in school. ☐
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. ☐
- I will not engage in any on-line activity that may compromise my professional responsibilities. ☐
- **The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:**
- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. ☐
- I will not use personal email addresses on the school ICT systems. ☐
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes. ☐
- I will ensure that my data is regularly backed up. ☐
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. ☐
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work. ☐
- I will not disable or cause any damage to school equipment, or the equipment belonging to others. ☐
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy Where personal data is transferred outside the secure school network, it must be encrypted. ☐
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority. ☐
- I will immediately report any damage or faults involving equipment or software, however this may have happened. ☐
- **When using the internet in my professional capacity or for school sanctioned personal use:**
- I will ensure that I have permission to use the original work of others in my own work ☐
- Where work is protected by copyright, I will not download or distribute copies (including music and videos). ☐
- **I understand that I am responsible for my actions in and out of school:**
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school. ☐
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police. ☐

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer /
Governor / Guest
Name

Signed

Date

Appendix 3: Online safety training needs – self-audit for staff

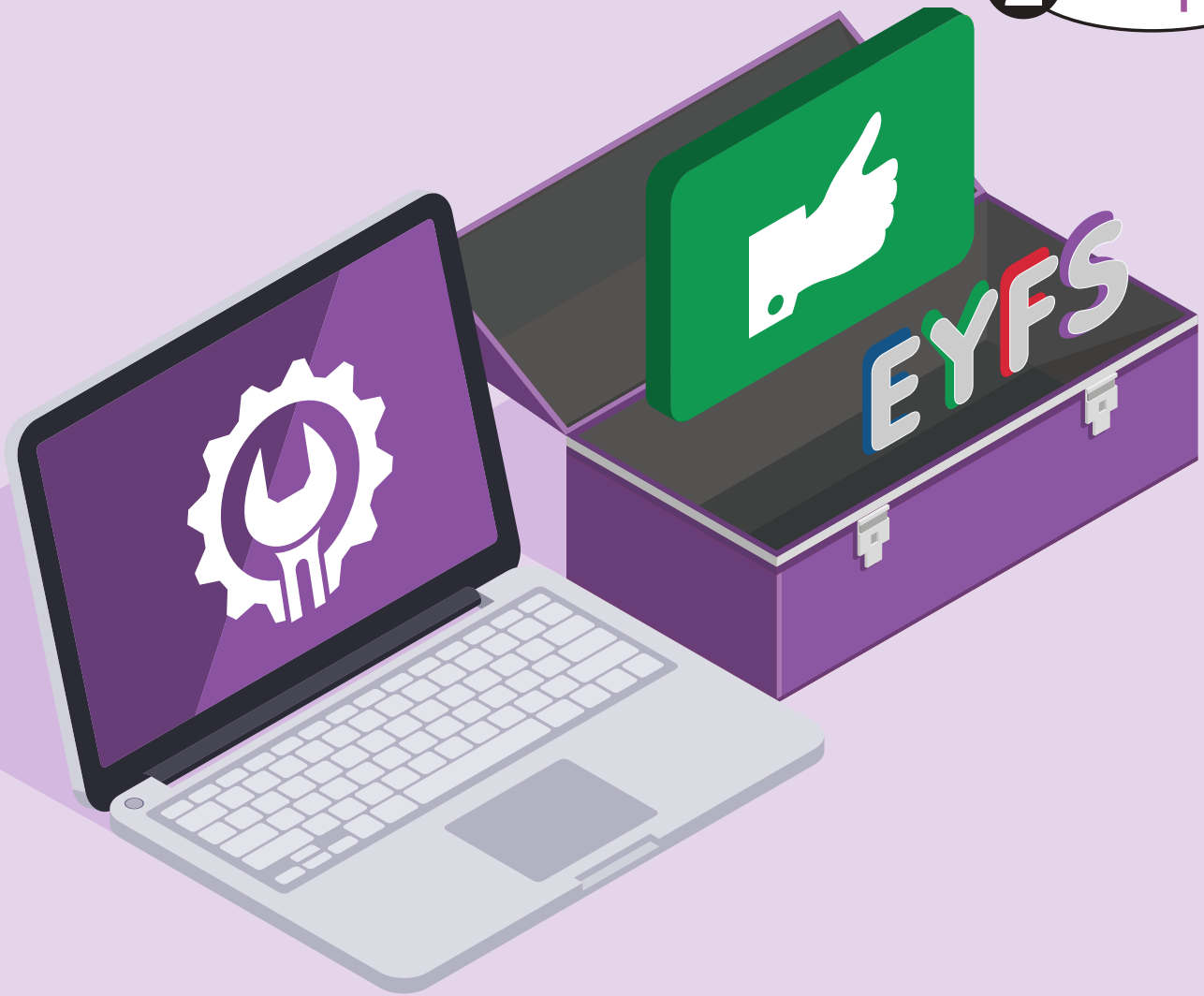
Adapt this audit form to suit your needs.

Online safety training needs audit	
Name of staff member/volunteer:	Date:
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 pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
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? Please record them here.	

Appendix 4: Online safety incident report log

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

2 simple

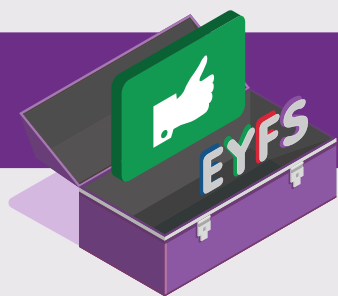


Acceptable Use Agreement (For EYFS)



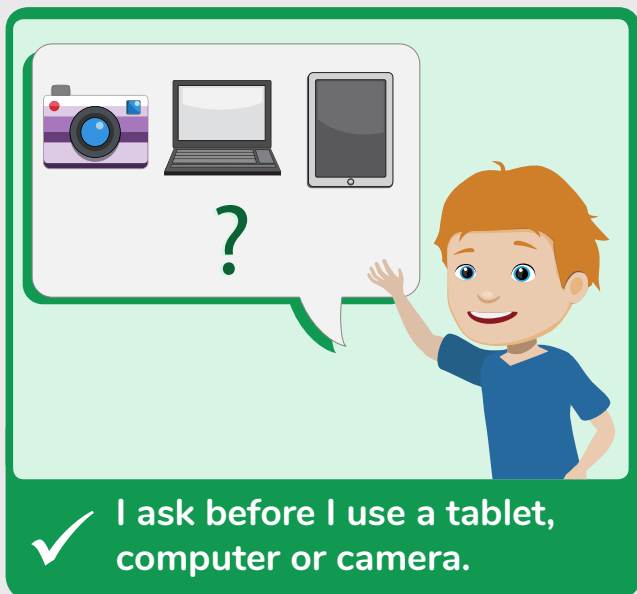
Computing Leader



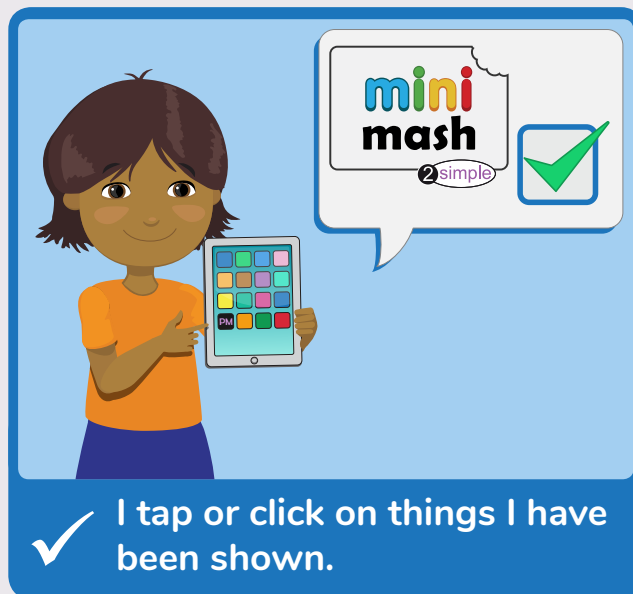


Acceptable Use Agreement

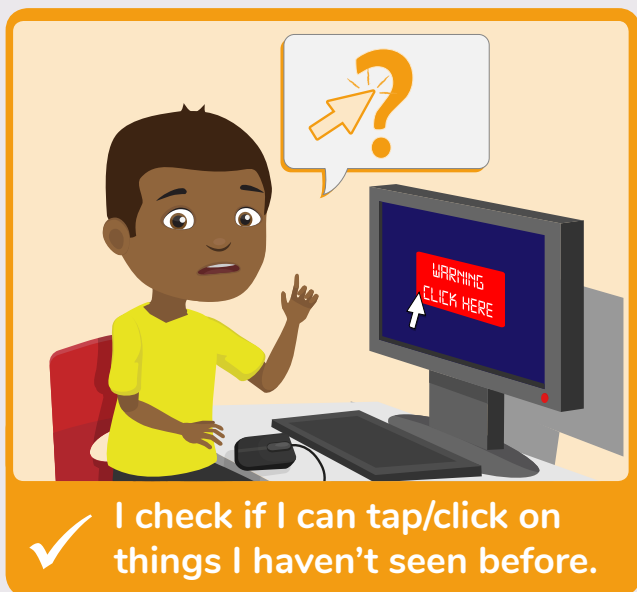
(For EYFS)



✓ I ask before I use a tablet, computer or camera.



✓ I tap or click on things I have been shown.



✓ I check if I can tap/click on things I haven't seen before.



✓ I tell a grown-up if something upsets me.

My Name:

Class:

Parent/Carer Signed:

Today's Date: