

# Cherry Tree Primary School



## ESAFETY POLICY

Current Version	March 2017
Approved by Governors	21 <sup>st</sup> March 2017
Reviewed by	Mary Fraser / Andy Feeley
Consulted	ICT Coordinator Staff
Review date	March 2018

## **Safety Audit**

This quick self-audit will help the senior leadership team assess whether the e-safety basics are in place.

Has the school an E-safety Policy that complies the latest guidance?	Yes
Date of lastest review:	March 2017
The Policy was agreed by governors on :	21 <sup>st</sup> March 2017
The Policy is available for staff:	On the Teaching Drive
And for parents at:	On the website
The Designated Child Protection Coordinator is:	Andrew Feeley
The E-safety / Computing Cordinator is:	Iain Shaw
Has Esafety training been provided for staff?	Yes
Has Esafety training been provided for pupils?	Yes
Do parents sign & return <ul style="list-style-type: none"><li>• An agreement that their child will comply with the School Esafety rules?</li><li>• The Acceptable User Policy (AUP) for pupils ?</li><li>• An agreement that their children’s work &amp; pictures may be displayed on the internet.</li></ul>	Yes
Has the school got an AUP / Esafety Rules age appropriate for pupils?	Yes
Is the AUP / Essafety rules displayed in all rooms with computers?	Yes
Internet access is provided by an educational Internet service provider and complies with DfES requirements for safe and secure access?	Yes
Has an ICT security audit been initiated by SMT, possibly using external expertise?	Yes
Is personal data collected, stored and used according to the principles of Data Protection Act?	Yes

<b>Key Members of staff</b>	
Executive head	Andrew Feeley
Head of School	Mary Fraser
Esafety / Computing Coordinator	Iain Shaw
Designated Child Protection Coordinator	Andrew Feeley
Linked Governor	Martin Rostron
Member of TA staff	Lynette Pulford

This policy outlines our purpose in providing e-mail and access to the Internet at **Cherry Tree Primary School** and explains how the school is seeking to avoid the potential problems that unrestricted Internet access could give rise to. It is not the intention of the policy to be unnecessarily restrictive. The aim of the policy is to ensure there is a framework of control in place.

The school currently purchases internet, email and web filtering through Bolton Local Authority. The server is bought from and maintained by the LA. The responsibility for ensuring that filtering systems and anti-virus / malware systems are up to date and fit for purpose sits within the remit of the SLA and school does not have the ability to check these ourselves. If the service provider changes, this policy will need to be updated.

### INTERNET ACCESS IN SCHOOL

Providing access to the Internet in school will raise educational standards and support the professional work of staff.

Teachers will have access to the Internet offering educational resources, news and current events they will also be able to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LA and DfES.

The Internet is being used to enhance the school's management information and business administration systems.

Pupils will have access to the Internet offering educational resources, news and current events. There will be opportunities for discussion with experts in many fields and to communicate and exchange information with students and others world-wide.

All staff (including teachers, supply staff and classroom assistants) and any other adults involved in supervising children accessing the Internet will be provided with the School Internet Access Policy and will have its importance explained to them.

Parents will be drawn to the Policy by letter and online within the ESafety section of the schools' web site.

### USING E-MAIL

All staff are strongly advised **NOT** to use or share their personal email account for school and therefore are issued with their own professional email which they will use appropriately to communicate with colleagues, parents, pupils and schools external services.

Staff should be aware the internet traffic maybe monitored and traced to the individual device or login. Discretion and professional conduct is essential. All email and electronic communication can be monitored at all times and could be open to investigation should the need arise by the Head of School with the support of Bolton Schools ICT Unit (SICT)

### INTERNET ACCESS AND HOME/SCHOOL LINKS

Parents will be informed that pupils are provided with supervised Internet access as part of their lessons. We will keep parents in touch with future ICT developments by newsletters and the school web site.

ESafety will be taught to all pupils as focused lessons every Autumn term and referred to then throughout the year. Sessions will be taught using age appropriate resources and cover the following areas: Email, SMS Messaging, Social Networking and Cyber Bullying. All children within these sessions will agree to their own Acceptable Users Policy. A most important element of our AUP / Esafety Rules is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Esafety assemblies will be held throughout the year where appropriate.

If a reported incident arises, staff will log the event with the Esafety / Computing Co-ordinator, staff will be informed and if appropriate a letter will be sent home to inform parents and a discussion to take place with all parties.

Parents' attention will be drawn to the school Esafety policy in newsletters, assemblies and on the school website. A series of parent workshops will be held throughout the year to support parents with e-safety and build strong partnership between parents, pupils and staff.

### USING INFORMATION FROM THE INTERNET

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the Internet is intended for an adult audience, much of the information on the Internet is not properly audited/edited and most of it is copyright.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true;
- When copying materials from the Web, pupils will be taught to observe copyright;
- Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.
- Pupils will be taught what Internet use is. The need for reliable information and given clear learning objectives for Internet use from the staff.
- Pupils will be educated in the effective use of Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age. In order to minimise the risk of children accessing harmful sites, staff to predetermine appropriate web links and add to a resource area the children can access.

If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will wish to respond to the situation quickly and on a number of levels

- Staff will log the event with the Esafety / Computing Co-ordinator;
- A letter will be sent home to inform parents;
- Discussion to take place with all parties.

Serious incidents within school will be referred to the Designated Child Protection Officer in consultation with the Head of School and the pupil's class teacher.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the AUP / Esafety Rules which have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet by failing to follow the rules they have been taught and rules set within the acceptable users' policy; then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers and access to the Internet may be denied for a period of time.

### SOCIAL NETWORKING

Children's access to a range of social media is becoming part of their everyday Internet browsing e.g. Club Penguin accounts or Moshi Monsters, thus it is school's responsibility to raise awareness as to what their personal information is and the implications of sharing this online.

Where are sites that have specific age restrictions children should be made aware of this. If a pupil has such accounts **this is ultimately the parents' responsibly**. We feel that as part of Esafety lessons there should be an open discussion around such sites, where age restrictions and the implications of having such accounts are discussed. Schools should strive to raise awareness through parent meetings their responsibility when their children access such sites.

The element of how to set privacy settings MUST be included whenever discussing social media sites.

If there are concerns raised during these sessions the members of staff should go through the appropriate reporting procedure.

### MAINTAINING THE SECURITY AND SAFETY OF THE SCHOOL NETWORK

We are aware that connection to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons. As part of the ICT SLA agreement the school receives regular Anti-Virus software updates. However it is the schools duty to notify the LA if there is a possible virus risk.

Our internet access is purchased from BOLTON LA, and the school has a “fileserver” which acts as the schools server, this provides a service designed for pupils including a “firewall” filtering system intended to prevent access to material inappropriate for children;

Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils;

Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;

Staff to ensure that when searching the Internet for images all projectors and Smartboards to be turned off or use the freeze tool enabling a wider use of images banks;

If staff or pupils discover unsuitable sites the Computing co-ordinator will be informed. The URL (address) and content will be reported to the LA ICT support team;

If it is thought that the material is illegal, after consultation with the LA ICT support team, the site will be referred to the Internet Watch Foundation and the police;

Our AUP / Esafety Rules will be posted near computer systems;

The Head of School / Computing lead will ensure that the policy is implemented effectively.

### REMOTE ACCESS

Where a teacher has access to school equipment out of school hours, teachers are encouraged to use these systems reasonably and appropriately.

All staff to be trained on how to save their files to the school network, home shared files and remote access. Removable media such as memory sticks, laptops, PDAs and mobile phones should not be used to store any sensitive or personal data.

Any data that could identify students or staff should not be removed from your school’s network without necessary controls being in place. This includes emailing personal information to home PCs.

### **Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry

out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website through the signing of the annual home school agreement
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

## **Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (see [Privacy Notice section in the appendix](#))
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs) Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.

Staff must ensure that they

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. This includes locking the computer when away from it
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

The Personal Data Handling Policy Template in the appendix provides more detailed guidance on the school’s / academy’s responsibilities and on good practice.

## Communications

This is an area of rapidly developing technologies and uses. A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to school	✓*						✓*	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓*							✓
Taking photos on mobile phones / cameras		✓						✓
Use of other school mobile devices e.g. tablets, gaming devices (not personal devices)	✓				✓			
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails	✓				✓			
Use of messaging apps				✓				✓
Use of social media				✓		✓**		
Use of blogs	✓				✓			

\*Staff mobile phones must be kept in the staffroom or switched off. They may not be used in front of the children at any time or during lessons. Pupil mobile phones will be kept in the locked cupboards in the classroom or office during the school day and will only be allowed in school if the parent can demonstrate a need for the child to have it.

\*\* There is a school facebook account which is run and administered by the parents and not school.



User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			

On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. YouTube			X		

## Staff

## Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head teacher Principal	Refer to Local Authority Designated Officer & HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X	X				X
Inappropriate personal use of the internet / social media / personal email		X				X		
Unauthorised downloading or uploading of files		X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X				X		
Careless use of personal data e.g. holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules		X						X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X						X

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X					X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					X
Actions which could compromise the staff member's professional standing		X						X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X						X
Using proxy sites or other means to subvert the school's / academy's filtering system		X						X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material		X	X	X				X
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X						X

## Key Responsibilities:

### Network Manager / Technical staff: (Currently server and internet / email managed by Bolton SICT at the LA)

The *Network Manager / Technical Staff / Co-ordinator for ICT / Computing* is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online technical requirements and any Local Authority / other relevant body Online Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are kept secure and changed if need be. Users with access to the 'office' drive (SLT) will have passwords changed regularly.

- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix “Technical Security Policy Template” for good practice)
- that they keep up to date with online technical information in order to effectively carry out their Online role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Executive Head teacher / Safeguarding governor; Computing subject for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school / academy policies

## Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online matters and of the current school Online policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the *Headteacher / Computing lead / Safeguarding governor* for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems*
- Online issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## Designated Safeguarding Lead

should be trained in Online issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

(nb. it is important to emphasise that these are child protection issues, not technical issues, simply which the technology provides additional means for child protection issues to develop. Some schools may choose to combine the role of Child Protection Officer / Safeguarding Officer and Online Officer)

## Students / pupils:

- are responsible for using the *school* digital technology systems in accordance with the Student / Pupil Acceptable User Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold

copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online practice when using digital technologies out of school and realise that the *school's* Online Policy covers their actions out of school, if related to their membership of the school

## **Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / blog and information about national / local online safety campaigns / literature*. Parents and carers will be encouraged to support the *school* in promoting good online practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / blog and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)





## **Community Users**

Community Users who access school systems / website / blog as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems. ([A Community Users Acceptable Use Policy Template can be found in the appendices.](#))

**It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor BOLTON LA can accept liability for the material accessed, or any consequences thereof.**

**APPENDIX 1 – Acceptable use policies**

**EYFS Acceptable Use Policy**

 My Learning	<ul style="list-style-type: none"> <li>• I will use school devices (PCs, laptops, tablets/ ipads) for my learning.</li> <li>• I will ask a teacher before using a device and ask for help if I can't work the device.</li> <li>• I will only use activities that a teacher has told or allowed me to use.</li> <li>• I will ask a teacher if I am not sure what to do or I think I have done something wrong.</li> <li>• I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.</li> </ul>
 My Online Safety	<ul style="list-style-type: none"> <li>• I will always use what I have learned about Online Safety to keep myself safe.</li> <li>• I will tell a teacher if I see something that upsets me on the screen.</li> </ul>
 Using the Internet @school	<ul style="list-style-type: none"> <li>• I will only use the internet when the teacher says I can.</li> <li>• I will only go on websites that my teacher allows me to.</li> <li>• I will tell my teacher if I go on a website by mistake.</li> </ul>
 Using the Internet @home	<ul style="list-style-type: none"> <li>• I will tell a trusted adult if I see something that upsets me on the screen.</li> </ul>

I understand that these rules help me to stay safe and I agree to follow them.  
 I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

\_\_\_\_\_  
**Child's Signature**

**EYFS Parents / Carers:**

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

**I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.**





---

**Parent/Carer's Signature**

---

**Date**

## Year 1 and Year 2 Acceptable Use Policy

 My Learning	<ul style="list-style-type: none"> <li>• I will use school devices (PCs, laptops, tablets/ ipads) for my learning.</li> <li>• I will ask a teacher before using a device and ask for help if I can't work the device.</li> <li>• I will only use activities that a teacher has told or allowed me to use.</li> <li>• I will ask a teacher if I am not sure what to do or I think I have done something wrong.</li> <li>• I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.</li> </ul>
 My Online Safety	<ul style="list-style-type: none"> <li>• I will always use what I have learned about Online Safety to keep myself safe.</li> <li>• I will tell a teacher if I see something that upsets me on the screen.</li> </ul>
 Using the Internet @school	<ul style="list-style-type: none"> <li>• I will only use the internet when the teacher says I can.</li> <li>• I will only go on websites that my teacher allows me to.</li> <li>• I will tell my teacher if I go on a website by mistake.</li> </ul>
 Using the Internet @home	<ul style="list-style-type: none"> <li>• I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details)</li> <li>• Where I have my own username and password, I will keep it safe and secret.</li> <li>• I will tell a trusted adult if I see something that upsets me on the screen.</li> </ul> <p><b>My use of Social Media and Gaming</b></p> <ul style="list-style-type: none"> <li>• I understand that certain sites and games have age restrictions to keep me safe.</li> <li>• I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.</li> </ul>

I understand that these rules help me to stay safe and I agree to follow them.  
 I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

I understand that these rules, help me to stay safe and I agree to follow them.  
 I also understand that if I break the rules I might not be allowed to use school computing equipment.

\_\_\_\_\_  
**Child's Signature**

\_\_\_\_\_  
**Date**



## **Key Stage 1 Parents / Carers:**

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

**I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.**




---

**Parent/Carer's Signature**

---

**Date**

## Year 3 and Year 4 Pupils School Acceptable Use Policy

 <p>My Learning</p>	<ul style="list-style-type: none"> <li>• I will use school devices (PCs, laptops, tablets/ iPads) for my learning.</li> <li>• I will ask a teacher before using a device and ask for help if I can't work the device.</li> <li>• I will only use activities that a teacher has told or allowed me to use.</li> <li>• I will ask a teacher if I am not sure what to do or I think I have done something wrong.</li> <li>• I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.</li> <li>• When logging on using my own username and password, I will keep it safe and secret.</li> <li>• I will save only school work on the school computer and will check with my teacher before printing.</li> <li>• I will log off or shut down a computer when I have finished using it</li> </ul>
 <p>Using the Internet @school</p>	<ul style="list-style-type: none"> <li>• I will only visit sites that are appropriate to my learning at the time</li> </ul> <p><b>My School Accounts</b></p> <ul style="list-style-type: none"> <li>• I will keep my username and password safe and secure - I will not share it.</li> <li>• I will not try to use any other person's username and password.</li> <li>• I understand that I should not write down or store a password where it is possible that someone may use it.</li> </ul> <p><b>My role as a Digital Citizen.</b></p> <ul style="list-style-type: none"> <li>• I will report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult.</li> <li>• I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.</li> </ul>
 <p>Using the Internet @home</p>	<ul style="list-style-type: none"> <li>• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details)</li> <li>• I will immediately report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies e.g.: CEOP, Childnet, Childline, Barnardos</li> </ul> <p><b>My Communications</b></p> <ul style="list-style-type: none"> <li>• I will be aware of the "SMART" rules, when I am communicating online.</li> <li>• I will be polite and responsible when I communicate with others.</li> <li>• I will not use inappropriate language and I understand that others may have different opinions.</li> </ul> <p><b>My use of Social Media and Gaming</b></p> <ul style="list-style-type: none"> <li>• I understand that certain sites and games have age restrictions to keep me safe.</li> <li>• I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.</li> </ul>

## Year 3 and Year 4 Pupils School Acceptable Use Policy

I understand that the school also 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).

I understand that these rules help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

---

**Child's Signature**

### **Year3 & Year4 Parents / Carers:**

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

**I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.**




---

**Parent/Carer's Signature**

---

**Date**

## Year 5 and Year 6 Pupils Acceptable Use Policy

 <p>My Learning</p>	<ul style="list-style-type: none"> <li>• I will use school devices (PCs, laptops, tablets/ ipads) for my learning.</li> <li>• I will ask a teacher before using a device and ask for help if I can't work the device.</li> <li>• I will only use activities that a teacher has told or allowed me to use.</li> <li>• I will ask a teacher if I am not sure what to do or I think I have done something wrong.</li> <li>• I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.</li> <li>• When logging on using my own username and password, I will keep it safe and secret.</li> <li>• I will save only school work on the school computer and will check with my teacher before printing.</li> <li>• I will log off or shut down a computer when I have finished using it.</li> </ul>
 <p>Using the Internet @school</p>	<ul style="list-style-type: none"> <li>• I will only visit sites that are appropriate to my learning at the time</li> </ul> <p><b>My School Accounts</b></p> <ul style="list-style-type: none"> <li>• I will keep my username and password safe and secure - I will not share it.</li> <li>• I will not try to use any other person's username and password.</li> <li>• I understand that I should not write down or store a password where it is possible that someone may steal it.</li> </ul> <p><b>My role as a Digital Citizen.</b></p> <ul style="list-style-type: none"> <li>• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult.</li> <li>• I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.</li> <li>• I will not take or distribute images of anyone without their permission.</li> </ul>
 <p>Using the Internet @home</p>	<ul style="list-style-type: none"> <li>• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details)</li> <li>• If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.</li> <li>• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies e.g.: CEOP, Childnet, Childline, Barnardos.</li> </ul> <p><b>My Communications (Including texting and messaging)</b></p> <ul style="list-style-type: none"> <li>• I will be aware of "stranger danger", when I am communicating online.</li> <li>• I will be polite and responsible when I communicate with others.</li> <li>• I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.</li> </ul> <p><b>My use of Social Media and Gaming</b></p> <ul style="list-style-type: none"> <li>• I understand that certain sites and games have age restrictions to keep me safe.</li> <li>• I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.</li> </ul>

I understand that the school also 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).

I understand that these rules, help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

---

**Child's Signature**

### **Year5 & Year6 Parents / Carers:**

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

**I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.**

---

**Parent/Carer's Signature**

---

**Date**

## Staff (and Volunteer) Acceptable Use Policy Agreement Template

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

### This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

### Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online in my work with young people.

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 (e.g. laptops, email, blog etc.) out of school, and to the transfer of personal data (digital or paper based) 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 not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 / blog it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / 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 mobile 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 also follow any additional rules set by the *school* about such use. 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 hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- 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 (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / 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 / academy 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 the *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 off the premises and my use of personal equipment on the premises 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 as set out in the disciplinary policy. 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 Name

Signed

Date

## Acceptable Use Agreement for Community Users Template

### This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

### Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 install or attempt to install programmes of any type on a school device, nor will I



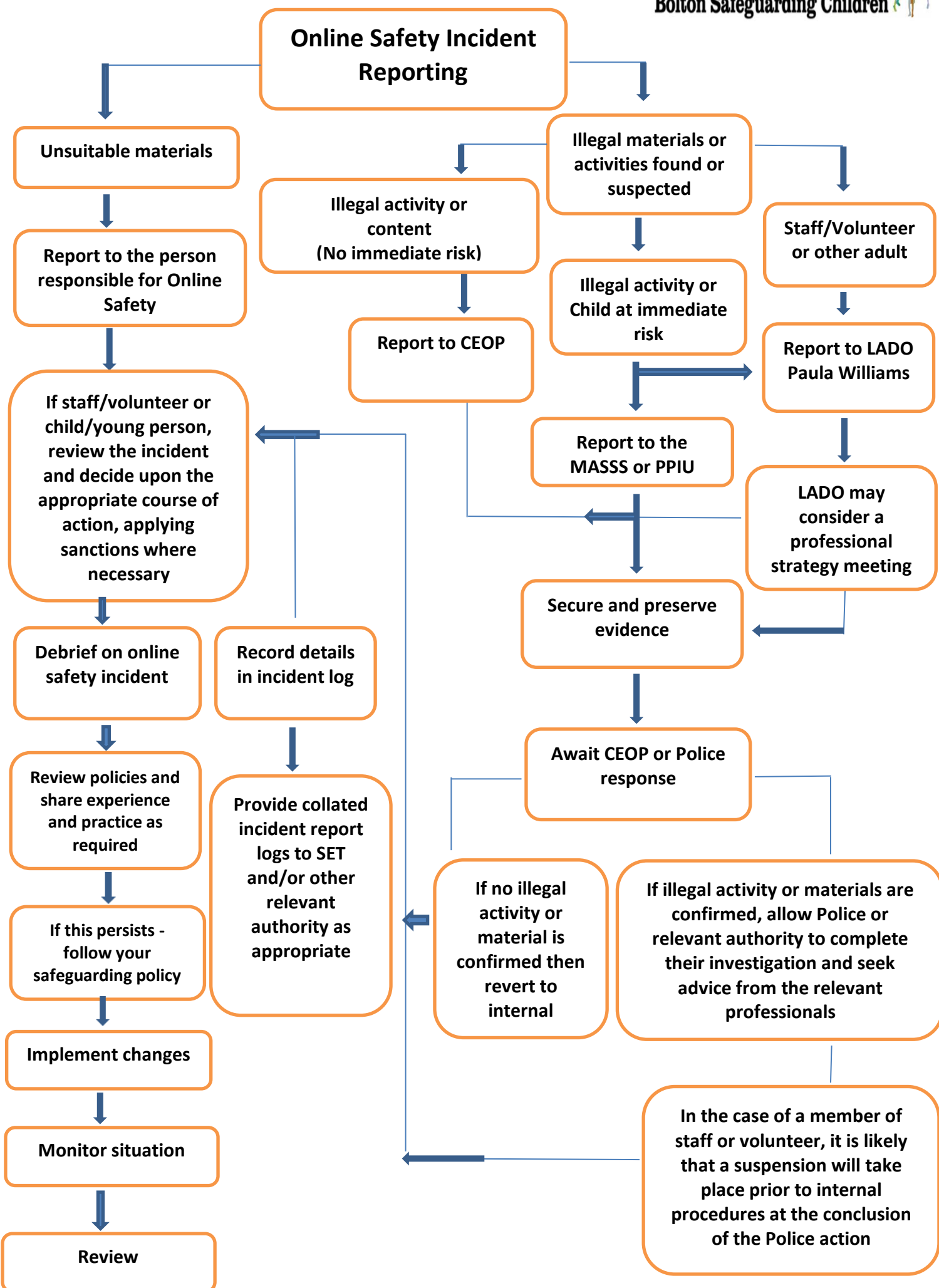
try to alter computer settings, unless I have permission to do so.

- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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 if I fail to comply with this Acceptable Use Policy, the school has the right to remove my access to school systems / devices

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.

**Print Name / Signature**

**Date**



## Support Contacts for Bolton Schools



### **SET – Safeguarding in Education Team:**

- Jacqui Parkinson – Safeguarding in Education Officer – 01204 337472
- Natalie France – Safeguarding Education Social Worker – 01204 331314

**LADO:** Paula Williams - 01204 337474

**Bolton's MASSS** – 01204 331500

**Police protection investigation unit** – 0161 856 7949

**Community Police** - 101

**EXIT Team** – 01204 337195

**Bolton Safeguarding Children's Board:** Shona Green – 01204 337964

If there is an ICT network issues contact your school ICT provider.

If your provider is Bolton School ICT Unit – contact 01204 332034 or [contact@sict.bolton.gov.uk](mailto:contact@sict.bolton.gov.uk)