The Gates Primary School Westhoughton

Online Safety
September 2025
Mrs S Jarrett

Scope of the Policy

The regulation and use of technical solutions to safeguard children are important but must be balanced with teaching the necessary skills to enable pupils to take responsibility for their own safety in an ever changing digital world. The National Computing Curriculum states that children should be able to use technology safely, respectfully, and responsibly keeping personal information private, recognise acceptable or unacceptable behaviour and identify a range of ways to report concerns about content and contact. Children's safety is paramount and they will receive the help, guidance and support through the whole curriculum to enable them to recognise and avoid online risks and to build their resilience. During the delivery of the curriculum staff will reinforce and consolidate safe online learning

This policy applies to all members of the school community who have access to and are users of school ICT systems and online resources, both in and out of school.

The school will deal with incidents as outlined within this policy, within the remit of their safeguarding, behaviour and anti-bulling policies (and others when applicable).

Roles and Responsibilities

Headteacher:

The Headteacher has a duty of care for ensuring the day to day safety (including Online) of all members of the school community.

The role of the Headteacher will include:

- ensuring that all members of the school community understand and acknowledge their responsibilities in the event of a serious online allegation being made (**Appendix 1**)
- ensuring that all relevant staff receive suitable training to enable them to carry out their safeguarding responsibilities within the remit of the Online Safety Policy
- ensuring that the Online Safety Policy is accessible to the wider School Community (School website)
- meeting at regular intervals with the Computing Lead to ensure the implementation of this policy (as outlined above). It is recommended that regular subject leader time is allocated to fulfil the role
- ensuring there are opportunities to communicate up to date Online Safety information to the wider school community

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Anti-Bullying and Behaviour Policy.

Governors:

Governors are responsible for the approval of this Online Safety Policy and for reviewing its effectiveness. This will be carried out by the Governing board, receiving regular information about online incidents and monitoring reports.

Where appointed, the role of the Online/safeguarding Governor will include:

- meetings with the Computing lead where appropriate
- regular monitoring of the Online Incident Log/CPOMS** (which will include anonymous details of Online Incidents Report Log **appendix 4**)
- ensuring robust technical support is in place to keep systems safe and secure
- regular monitoring of filtering
- reporting to the Governing board
- attending training for online safety where appropriate

Safeguarding Lead

The Safeguarding Lead is responsible for taking any necessary action as per the Online Safety Incident reporting flowchart (**Appendix 1**).

They will be trained in online issues and acknowledge and understand the potential for serious child protection / safeguarding issues that arise from, but not limited to

- sharing of personal data
- accessing illegal / inappropriate materials
- exposure to inappropriate online content
- inappropriate contact with adults/strangers
- potential or actual incidents of grooming
- sexting
- cyber-bullying

In the event of a child protection or safeguarding incident pertaining to the above, the safeguarding lead will refer to appendix 1.

Computing Lead

The Computing Lead is responsible for the management of online issues and takes a leading role in establishing and reviewing the school Online Safety Policy.

The role of the Computing Lead includes:

- providing advice for staff and signpost relevant training and resources
- liaising with relevant outside agencies
- liaising with relevant technical support teams
- collating and reviewing reports of Online Incidents (**CPOMS**/A**ppendix 4**)
- meeting regularly with Headteacher to discuss issues and subsequent actions
- taking action in response to issues identified
- communicating up-to-date Online Safety information to the wider school community

School Staff

It is essential that all staff

- understand and acknowledge their responsibilities as outlined in this Policy
- have read, understood and signed the Staff Acceptable Use Policy (Appendix 3)
- keep up to date with the Online Safety Policy as part of their CPD

- have an up-to-date awareness of online matters pertinent to the children that they teach/have contact with
- report concerns and log incidents (A**ppendix 4 /**CPOMS**)
- when addressing any suspected misuse or Online Safety Issue, refer to appendix 1 or appendix 4, depending on the severity
- ensure that all digital communications with the School Community are on a professional level and only carried out using official school approved systems
- apply this Online Safety Policy to all aspects of the Curriculum
- share, discuss and ensure the children understand and acknowledge their responsibility to follow their age-appropriate Acceptable Use Policy
- are good role models in their use of all digital technologies
- are vigilant in monitoring how pupils use digital technologies and access online content whilst in their care
- staff are permitted to use artificial intelligence (AI) to support in their planning and teaching to support workload and wellbeing but agree to follow the guidelines outline in the schools AI policy.

It is accepted that from time to time, for purposeful/appropriate educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable with clear reasons for the need.

Technical support

The school's technical infrastructure must be secure and actively reduces the risk of misuse or malicious attack.
To facilitate this, school has purchased support from Bolton Schools ICT.
The role includes:

- ensuring that detected risks and/or misuse is reported to the Headteacher at school
- ensuring that schools are informed of any changes to guidance or any planned maintenance
- school technical systems will be managed and reviewed annually in ways that ensure that the school meets recommended technical requirements
- all users will have clearly defined access rights to school technical systems and devices
- all school network users will be assigned an individual username and password at the appropriate level of access needed for their role
- ensuring internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list
- content lists are regularly updated and internet use is logged and regularly monitored
- there is a clear process in place to deal with requests for filtering changes
- provide a platform where school should report any content accessible in school but deemed inappropriate
- ensuring appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software (**Appendix 2**)
- the use of Fastvue will send alerts to the school if a child is searching or attempting to access inappropriate content online.

Pupils

The children's learning will progress through a broad, effective and relevant Online Safety curriculum.
A pupils learning journey will be holistic in that it will include, but is not limited to their online reputation, online bullying and their health and wellbeing.

It is essential that all pupils should:

- understand, acknowledge and adhere to their age-appropriate Acceptable Use Policy (**Appendix 3**)
- be able to recognise when something makes them feel uncomfortable (butterfly feeling) and know how to report it
- accept their responsibility to respond accordingly to any content they consider as inappropriate
- understand the importance of being a responsible digital citizen and realise that the school's Online Safety Policy applies to their actions both in and out of school
- know that school will take action in response to any breach of the Online Safety Policy
- the use of Fastvue will send alerts to the school if a child is searching or attempting to access inappropriate content online.

Parents / Carers / Responsible adults

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's on-line usage. Due to the ever evolving Digital World, adults can sometimes be unsure of how to respond to online risks and issues. They may also underestimate how often pupils encounter potentially harmful and inappropriate online material.
Therefore, it is essential that all adults should:

- promote safe and responsible online practice and must support the school by adhering to the school's Safeguarding and Online Safety Policy in relation to digital and video images taken whilst on school premises or at school events
- understand, acknowledge and adhere to their child's Acceptable Use Policy (**Appendix 3**)
- understand, acknowledge and ensure that their child adheres to school procedure relating to their use of personal devices whilst on school grounds

To support the school community, school will provide information and awareness through, but not limited to:

- letters, newsletters, website links, publications, external agencies
- Parents / Carer workshops
- high profile events / campaigns e.g. Safer Internet Day

Visitors entering school

It is essential that school apprise visitors of all relevant policies pertaining to their visit and contact with pupils.

Useful Information

Safeguarding

In the event of a Safeguarding infringement or suspicion, appendix 1 must be followed with consideration of the following:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported
- Conduct the procedure using a computer that will not be used by pupils and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the investigation, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
- Record any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed (except in the case of images of child sexual abuse – see below)
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include: incidents of 'grooming' behaviour the sending of obscene materials to a child adult material which potentially breaches the Obscene Publications Act criminally racist material other criminal conduct, activity or materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the Safeguarding Lead for evidence and reference purposes.

Data Protection

Personal and sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Schools are audited regularly regarding how they handle their data, for further information please refer to school Data Protection Policy.

Communications

When using communication technologies the school considers the following as good practice:

- The Office 365 school email service is safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school
- When accessing emails out of the schools setting, staff will only be able to access their schools emails using Microsoft Multifactor Authentication app.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- When conducting virtual meetings staff will do so in a professional manner, dress appropriately and ensure the area the meeting is taking place is appropriate.
- When children are blogging they will be kind and respectful to other children and adult, not post any personal information about themselves or others and will report anyone else that is not conducting themselves in this manner.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

The school's use of social media is to promote the ethos of the school. It is the responsibility of all staff to ensure that the content they upload is for professional purposes only, be compliant with the school policies and protect the identity of pupils.

Home and Remote Learning - Seesaw

Seesaw will act as an online portfolio for children, providing them with the platform to capture practical learning which was previously unachievable - our pupils will now be able to capture and record pictures, videos and sound recordings of their learning. When using Seasaw for home and remote learning children agree to submit appropriate posts as discussed in class. Inappropriate posts include insulting, hurtful, insensitive comments as well as inappropriate images. All posts will be filtered by the class teachers - all posts will always be moderated and approved by staff before being made visible by the rest of the class. In addition, parents will only be able to see posts which their own child has been tagged in. Staff will be responsible in ensuring that any vulnerable children are protected from being photographed and visible in group-tagged in group posts. Children's Seesaw logins should be kept safe and not shared with other students/people.

Home and Remote Learning – Teacher posts

Teachers agree to conduct themselves in an professional manner as they would in the classroom. Teachers should always ensure they record lessons in an appropriate setting in appropriate clothing. Parents are required to follow the agreed protocol of contacting the office if they have any concerns. They should not use their children's Seesaw profiles to contact class teachers.

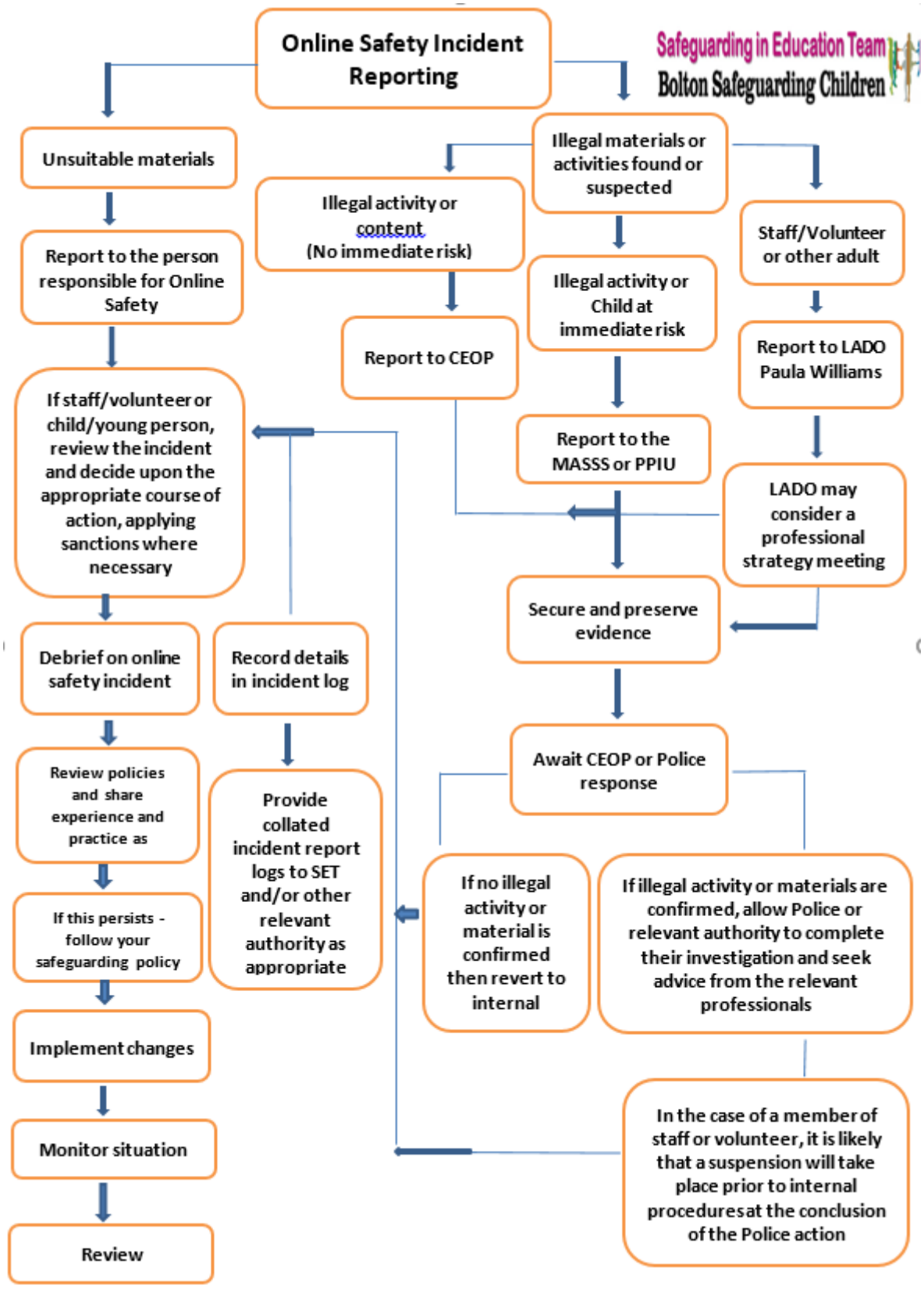
Schedule of Monitoring and Review

The implementation of this Online Safety Policy will be monitored by the:	Sean Doherty Sarah Jarrett Governors Safeguarding Lead
The school will monitor the impact of the policy using:	Logs of reported incidents Monitoring logs of internet activity (including sites visited) Internal monitoring data for network activity Surveys / questionnaires of stakeholders – staff, pupils, parents
Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group at regular intervals:	Termly where appropriate

Should serious Online incidents take place, the following external persons / agencies should be informed:	Headteacher School Safeguarding Lead LADO Police **See Appendix 1**

Appendices

Appendix	
1	Online Safety Incident Flowchart
2	School Technical Security Overview
3	AUP documents – Staff / Pupils / Visitors
4	Online Incident Report Log


Online Safety Incident Reporting
Safeguarding in Education Team
Bolton Safeguarding Children
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as
If this persists - follow your safeguarding policy
Implement changes
Monitor situation
Review
Record details in incident log
Provide collated incident report logs to SET and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal activity or content (No immediate risk)
Report to CEOP
Illegal activity or Child at immediate risk
Report to the MASSS or PPIU
Staff/Volunteer or other adult
Report to LADO Paula Williams
LADO may consider a professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professionals
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the Police action

Support 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 01024 332034 or contact@sict.bolton.gov.uk

App 2

ICT Guidance for OfSTED inspection

It has been brought to our attention that during recent OfSTED inspections, questions have been asked about procedures schools are using for internet filtering and security.
We produced the notes below to assist one colleague with this and the information seemed to be helpful when answering the inspector's questions.
Therefore, I am sharing this to hopefully be of assistance should your school be inspected.
Should you need any further assistance during inspection regarding ICT issues, please contact the unit and we will assist wherever possible.

For Bolton schools subscribing to Bolton Schools ICT (Bolton SICT) Broadband services, internet access is via the local authority maintained Wide Area Network.
We use a central internet filtering system for all schools.
This is an industry standard solution, Sophos Universal Threat Management, the product incorporates the IWF standards.
We have this configured as per DFE guidelines, see following technical blog post:

https://technical.bolton365.net/internet-filtering/

The system can also be deployed at school level if required, but the standard configuration has distinct filtering levels for staff and pupils.

Filtering change requests are online and are only accepted from authorised users. Any changes are security checked before implementation.

The system provides Bolton SICT with full monitoring and reporting, these reports are available to schools when requested.

Bolton Schools ICT Broadband service also includes:

- *Email content filtering*
- *Email anti spam*
- *Secure email facilities – Multi Factor Authentication*
- *Full anti virus*
- *Encrypted document exchange*
- *2 factor remote access*
- *Industry standard firewalls to protect both WAN and school LANs*

Bolton School ICT staff that maintain these systems are all minimum Microsoft qualified and have many years industry experience.

The Inspectors have also indicated that pupils from Year 1 onwards should be using individual logins to allow monitoring of computer usage.
Some schools are already doing this, from EYFS, for network, Purple Mash and blog logon, using a four digit password.

If your school requires this facility, please contact the unit via email at contact@sict.bolton.gov.uk
For devices, such as iPads, that do not do not use network logins, we are currently looking at ways of user authentication to provide monitoring.

Yours sincerely

Sam Stoneley
Schools ICT Unit Manager
Tel: 01204 332034 Fax: 01204 332235 Email: Sam.Stoneley@sict.bolton.gov.uk

App 3

EYFS Acceptable Use Policy

 My Learning	• I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.
 My Online Safety	• I will always use what I have learned about Online Safety to keep myself safe. • I will tell a teacher if I see something that upsets me on the screen.
 Using the Internet @school	• I will only use the internet when the teacher says I can. • I will only go on websites that my teacher allows me to. • I will tell my teacher if I go on a website by mistake.
 Using the Internet @home	• I will tell a trusted adult if I see something that upsets me on the screen.

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

Year 1 and Year 2 Acceptable Use Policy

 My Learning	• I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.
 My Online Safety	• I will always use what I have learned about Online Safety to keep myself safe. • I will tell a teacher if I see something that upsets me on the screen.
 Using the Internet @school	• I will only use the internet when the teacher says I can. • I will only go on websites that my teacher allows me to. • I will tell my teacher if I go on a website by mistake.
 Using the Internet @home	• I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details) • Where I have my own username and password, I will keep it safe and secret. • I will tell a trusted adult if I see something that upsets me on the screen. **My use of Social Media and Gaming** • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.

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

_____

Year 3 and Year 4 Pupils School Acceptable Use Policy

 My Learning	• I will use school devices (PCs, laptops, tablets/ iPads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it.
 Using the Internet @school	• I will only visit sites that are appropriate to my learning at the time **My School Accounts** • I will keep my username and password safe and secure - I will not share it. • I will not 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 use it. **My role as a Digital Citizen.** • I will report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. • 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.
 Using the Internet @home	• 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) • 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 eg: CEOP, Childnet, Childline, Barnardos **My Communications** • I will be aware of the "SMART" rules, when I am communicating online. • I will be polite and responsible when I communicate with others. • I will not use inappropriate language and I understand that others may have different opinions. **My use of Social Media and Gaming** • I understand that certain sites and games have age restrictions to keep me safe.

	• I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.

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

Year 5 and Year 6 Pupils Acceptable Use Policy

 My Learning	• I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it.
 Using the Internet @school	• I will only visit sites that are appropriate to my learning at the time **My School Accounts** • I will keep my username and password safe and secure - I will not share it. • I will not 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. **My role as a Digital Citizen.** • 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. • 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. • I will not take or distribute images of anyone without their permission.
 Using the Internet @home	• 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) • 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.

	• 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. **My Communications (Including texting and messaging)** • I will be aware of "stranger danger", when I am communicating online. • I will be polite and responsible when I communicate with others. • I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. **My use of Social Media and Gaming** • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.

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

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**

Appendix4

ONLINE INCIDENT LOG

Details of ALL Online incidents to be recorded by the Online Lead within your School, this incident log will be monitored weekly by a senior member of staff.

Date & time	Name of child or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons