



BLENHEIM
SCHOOLS

Web Filtering & Monitoring Policy

Policy Folder: Safeguarding

Web Filtering & Monitoring Policy

Contents

1.0	POLICY STATEMENT	2
2.0	LEGAL AND POLICY FRAMEWORK	2
3.0	SCOPE OF THE POLICY	3
4.0	ROLES AND RESPONSIBILITIES	3
5.0	WEB USE AND POTENTIAL RISKS	4
6.0	WEB FILTERING SYSTEM	5
7.0	REPORTS AND CHECKS	5
8.0	MEETING THE FILTERING AND MONITORING STANDARDS FOR SCHOOLS AND COLLEGES	6
9.0	LOCAL ARRANGEMENTS FOR WEB FILTERING AND MONITORING.....	6

Terminology - Please note that the terms “our teams” and “team member/s” include everyone working with the people in Outcomes First Group’s services in a paid or unpaid capacity, including employees, consultants, agency staff and contractors.

1.0 POLICY STATEMENT

We are committed to ensuring that all children and young people we educate and care for are safeguarded at all times, both offline and online. Their safety is our highest priority and must remain central to everything we do. Accessing the internet and using social media is part of everyday life and provides many positive possibilities. However, it also carries significant risks to which some of the children and young people we educate and care for can be more susceptible than their peers. Those already at risk offline are more likely to be at risk online.

Educating our children and young people on how to use the internet safely is a vital part of the setting’s education provision. An effective whole-setting approach to online safety helps team members to protect and educate our children and young people and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. A key element is the implementation of effective web filtering and monitoring systems to help protect them from potentially harmful or inappropriate online content.

2.0 LEGAL AND POLICY FRAMEWORK

This policy focuses specifically on the web filtering and monitoring in place in children’s education and care settings to help protect children and young people. It must be read alongside and in addition to the setting’s:

- Safeguarding Policy
- Protecting Children from Radicalisation Policy and Guidance
- Child Exploitation Policy
- Mobile and Smart Technology Policy



And the Group's

- Staying Safe Online Policy
- Gaming Devices Best Practice Guidance
- AI Policy & AI Acceptable Use Policy

This policy is written in line with the relevant legislation, regulations and government guidance, including:

- [Keeping Children Safe in Education \(KCSiE\) 2025](#) (DfE)
- [Meeting digital and technology standards in schools and colleges](#) (DfE)
- [Generative AI Product Safety Expectations](#) (DFE)

It will be reviewed annually or whenever significant changes are made to national policy and legislation.

3.0 SCOPE OF THE POLICY

This policy applies to all of the school community, including governors, proprietors, senior leadership teams, all team members, parents/carers, visitors and community users who access the internet over the setting's wireless network. A child or young person using their own IT equipment at one of our sites over the Wi-Fi is within scope, however, only a default set of web-filtering rules would be applied.

We are not able to apply web filtering protection when devices are used outside of the Group's sites or when using Mobile Data Networks.

4.0 ROLES AND RESPONSIBILITIES

4.1 Governors and proprietors are required to do all that they reasonably can to limit children's exposure to online risks from the school's IT system, including:

- Ensuring that **all team members** undertake safeguarding and child protection training, (including online safety which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. The training should be regularly updated.
- Ensuring the setting has appropriate filters and monitoring systems in place, that are informed in part by the risk assessment required by the [Prevent Duty](#), and regularly review their effectiveness.
- Ensuring that the leadership team and relevant team members have an awareness and understanding of the appropriate online filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified;
- Consider the age, development range and number of children and young people and their needs, how often they access the IT system and the proportionality of costs versus safeguarding risks.
- The DfE's [filtering and monitoring standards](#) requires schools to:
 - identify and assign roles and responsibilities to manage filtering and monitoring systems
 - review filtering and monitoring provision at least annually



- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs
review the standards and discuss with IT and service providers what more needs to be done to support schools in meeting this standard. Please also see the DfE's [Plan technology for your school](#)
- Meet the [Cyber security standards for schools and colleges](#).
- Broader guidance on cyber security [Cyber security training for school staff](#)

4.2 The Designated Safeguarding Lead (DSL), appointed by the governors and proprietors in the school, should take lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. **This should be explicit in the role-holder's job description.**

The DSL/Safeguarding Lead will work closely with IT Services and providers to meet the needs of the setting and request system specific training and support as and when required. They will take lead responsibility for any safeguarding and child protection matters that are picked up through web filtering and monitoring systems in place.

DSLs and Safeguarding Leads working in integrated or joint sites must liaise regularly with each other. They must work closely and communicate frequently to ensure they are both aware of any concerns and that children are safeguarded effectively and consistently.

4.3 All team members are required to adhere to the Group's internal procedures relating to safeguarding and child protection and managing allegations as well as the Local Safeguarding Partnership's procedures.

4.4 Team members and visitors must not, under any circumstances, allow a child or young person to use their device, online account or hotspot or share any of their login details or passwords. This is for the safety and protection of the child/young person and the team member.

5.0 WEB USE AND POTENTIAL RISKS

The potential risks from online use are extensive and ever evolving, but can be categorised into four areas:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm
- Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

DFE has published [Generative AI Product Safety Expectations](#) to support schools to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in education.



6.0 WEB FILTERING SYSTEM

The Group operates a secure web filtering system on the internet link to the setting. This means that it safeguards as far as is possible the computers and internet use within the setting, and it also offers safeguards on every mobile phone and tablet used in the setting over the setting's Wi-Fi network. Web filtering and monitoring helps to keep children and young people safe from illegal content and help protect them from extremism online when using the setting's Wi-Fi, it is informed in part, by the risk assessment required by the Prevent Duty.

Oxford Montessori Schools uses Smoothwall Filtering and Monitoring.

All users should understand that the primary purpose of the use of the internet in a school context is educational. The web site categories that are blocked are to ensure the safety and well-being of young people.

The web filtering system does not safeguard the use of a mobile phone or tablet that is accessing the internet over mobile phone signals. Controls on a child or young person's device to safeguard web browsing will need to be agreed between the school and child/young person, their parent or carer and their social worker. Team members must ensure a risk assessment is in place for any other device in use by children or young people in the setting.

As part of the induction to school, the pupil and parents/carers/ those with parental responsibility are required to sign an IT user agreement (examples are included at Appendix A) which includes agreeing to ensure appropriate parental controls are on any devices used at school.

Social media website categories are blocked at Group level when children and young people access the internet within the school. Team members must also ensure that they refer to the *Mobile and Smart Technology Policy*.

7.0 REPORTS AND CHECKS

7.1 Monthly Reports

The DSL and the Headteacher or equivalent receive monthly reports of sites that have been blocked following attempted access.

The DSL/Safeguarding Lead will investigate attempted access of inappropriate sites that cause concern as soon as possible and take appropriate action. Attempted access of websites related to extremism will be referred appropriately in line with the [Prevent Duty](#) and local arrangements for reporting.

The monthly reports will be stored by the setting for a period of six months unless there are safeguarding concerns. If there are safeguarding concerns the information will be stored in line with statutory requirements for record retention.

7.2 Checks and tests

The Headteacher or equivalent will ensure arrangements are in place to regularly check the filtering and monitoring system is working as intended and adequately and that these checks are recorded. This includes testing the system to see if inappropriate websites can be accessed. The South West Grid for Learning's (SWGfL) [testing tool](#) can be used to check that, as a minimum, the filtering system is blocking access to: illegal child abuse material; unlawful terrorist content and adult content. I

The frequency of these tests is weekly and any risks highlighted in the setting's filtering and monitoring review, and any other risk assessments. It is expected that tests are carried out at least weekly, where heightened risks are identified, tests may need to be carried out more frequently. A written record of the checks must be kept.

8.0 MEETING THE FILTERING AND MONITORING STANDARDS FOR SCHOOLS

The following documents have been made available on the Blenheim Resources site to support our settings to meet the DfE [Filtering and monitoring standards for schools](#):

- A questionnaire/spreadsheet to help work through the standards to assess compliance.
- Annual school Online Safety Audit & Risk Assessment template
- A KCSiE annual update course that is mandatory for all Education team members and available to all team members in the Group.

Free online safety self-review tools can be found at: <https://360safe.org.uk/> and

9.0 LOCAL ARRANGEMENTS FOR WEB FILTERING AND MONITORING

All team members must be aware of the local arrangements for safeguarding relevant to the setting in which they work and the arrangements for keeping children and young people safe online. The arrangements for web filtering and monitoring at Oxford Montessori Schools are as follows:

HOW WILL OMS PROTECT CHILDREN UNDER THIS POLICY?

1. **FILTERING** - The process of controlling what can be accessed on our school network via the internet and excluding as much harmful content as possible.
2. **MONITORING** - The process of overseeing what attempts have been made to see restricted material or visit inappropriate websites, reporting on them and taking action to appropriately respond to those behaviours.
3. **TRAINING** - Training students to keep themselves safe online and training staff to understand the school's filtering and monitoring systems and knowing who to report to in the case of a digital safeguarding concern.



4. CYBER SECURITY - Defending school systems, network, hardware and software from malicious attack and putting systems in place to protect the data and personal information of anyone related to school, especially children but also including staff, contractors and visitors

FILTERING

OMS will take every measure to protect children online but also ensure that the filtering system does not unreasonably impact on learning. Children will also be encouraged to learn how to assess and manage risk for themselves.

Oxford Montessori Schools uses a Smoothwall firewall and content filter to block access to inappropriate content and social media platforms. It is active 24 hours a day.

Smoothwall will block attempts to access websites with content related to:

- abuse (all forms)
- terrorism/extremism/radicalisation (including police uploaded threat information)
- adult content, including gambling, violence and pornography
- bullying or offensive language or discrimination
- criminal activity
- Substance abuse
- Suicide/self harm

The following internet security protocols are in place:

* The Smoothwall firewall and content filter blocks access to inappropriate content and provides configurable monitoring and reporting capabilities to effectively manage the Schools' internet access.

* Every school network device and all school devices using OMS' wifi and internet access operate under a correctly configured software firewall. BYOD (Bring Your Own Device) accessing the school network have restricted and managed access to the internet via the school wifi and are within the firewall when using the school network. (Mobile phones and devices that access the internet via mobile network connections are not protected by the Smoothwall Firewall and Filter as traffic does not pass through the OMS network domain.)

* All Network Devices (eg. school laptops and desktops, printers, ipads etc.) will be known and recorded with their security features enabled, correctly configured within the wifi network and under the domain, with all security protocols up to date and activated within the Smoothwall firewall system.

* On setting up the Smoothwall system all default administrator passwords were disabled. This reduces significantly the possibility of remote access from unauthorised entities.



OMS blocks all social media sites but allows access to certain websites for educational purposes, for example YouTube may be accessible in specific classes at specific times for specific topics. A log is kept of any exceptions to the filtering system, any websites given access (even on a temporary basis) and the rationale behind that decision. A log is also kept of any websites that OMS has chosen to block and the reasons for that decision.

It is vital that the Smoothwall filtering system does not unreasonably impact on learning. Therefore if teachers require access to certain websites or certain subjects during specific times or in a particular period, we can arrange that through the Smoothwall system to allow appropriate access for learning. Teachers are required to put these requests in writing and confirmation of the access given and the criteria for use will be emailed back to them.

At OMS many of the computers used by staff and students are owned by the individuals and not the school. This BYOD set up means we cannot install embedded software restrictions on the computers and cannot filter as effectively at the https:// search level. To support the school in managing https:// searches our second line filtering is the Google proprietary system Google Safesearch. This works by analysing the search string and providing search results which prioritise safe responses.

No filtering system is 100 percent reliable so all OMS staff must be vigilant, observant and demonstrate a level of intrusion on a child's online activity that balances keeping them safe with infringing personal rights in a way that displays positive digital safeguarding practices.

MOBILE DATA

Mobile data is not subject to the same filtering as any traffic on Oxford Montessori's wifi or internet network. Mobile data can be accessed via mobile telephones or smart watches and use of mobile data gives children access to unfiltered content.

To combat the threat of mobile data, OMS collects all mobile phones from students on entry to school in the morning and returns them each evening when students leave the premises. No access is given during the day unless an urgent or emergency situation arises and then use is under strict supervision.

Smart watches are required to be configured to 'School Mode' during the academic day, which means they do not have internet access unless specific conditions are met, such as use to record performance in a PE lesson under the direct supervision of a teacher.

MONITORING

OMS will have effective monitoring strategies in place that meet the safeguarding needs of our schools. This will be overseen by the DSL/DDSL who have overall responsibility for the monitoring system and actions taken.

All staff will be trained on how to follow policies and procedures, to act on reports and concerns and to understand their role in the monitoring process.

As we are largely a BYOD school, OMS is not able to identify individual computers except by IP address. Nevertheless we have an active monitoring strategy.

- Smoothwall sends alerts to the DSLs if attempts are made to access concerning things, such as suicide sites or extreme radicalisation sites
- Full safeguarding reports are run on a monthly basis. This lists in full which sites are attempting to be accessed, by IP address, the date and time of access. The report is circulated to the DSL's, Proprietors and Admin Staff. A monitoring report is prepared listing all the attempts, detailing occurrences and indicating actions taken and by whom.
- All teachers will be trained to be vigilant. To maintain digital safety they will need to look over children's shoulders at what they are accessing and be aware if a child closes their laptop down or starts to fiddle with their power cable when staff are near, as that may be a concern.
- OMS produces reports and checks monitoring logs of traffic passing through the Smoothwall filter and firewall, detecting suspicious activity and ensuring the validity of rules and protocols to secure the OMS network domain access.
- Where possible individual computers and IP addresses will be recorded to identify users. It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.

TRAINING

Digital safeguarding is part of all safeguarding and induction training for all OMS staff.

When devising and reviewing our digital safeguarding policy we look at the risk profile of OMS' pupils, any relevant outside safeguarding influences (such as County Lines pressure), the digital resilience of pupils (which means how resourceful students will be at getting around our protections) and what decisions we make around the controls we put in place (for examples which websites we may choose to bar completely).



For students we have devised a robust teaching plan to help them stay safe online and to support them in navigating the intrusive and encompassing online world. We acknowledge this is a fast changing area and constant review is necessary. As part of the DSL/DDSL's responsibility, OMS' PHSEE/RHSE is carefully planned and well delivered to give children the tools to safeguard themselves as much as possible.

CYBER SECURITY

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

As part of this policy only authorised applications or programs can be installed or downloaded onto school network devices. A log will be kept of all authorised software and approval must be obtained from either the Principal (Katie Townsend) or Data Protection Officer (Teresa Andrews) before access to the software is made.

OMS has the following cyber security measures already in place or under review:

SOFTWARE MANAGEMENT

- * Any auto-run features that allow file execution on unauthorised applications are disabled on school devices
- * A log will be kept of all authorised software and applications running on OMS devices and authorisation will be required before any additional software/apps are downloaded or installed.

FIREWALL AND ANTI-MALWARE/VIRUS

- * Every school network device and all school devices using OMS' wifi and internet access operate under a correctly configured software firewall. BYOD devices accessing the school network have restricted and managed access to the internet via the school wifi and are within the firewall when using the school network.
- * The Smoothwall firewall's administrative interface is protected both with multi factor authentication and a small specified IP-allow list, combined with a managed password
- * The Smoothwall's firmware is up to date
- * Inbound unauthenticated connections are blocked by Smoothwall
- * Inbound traffic blocked by Smoothwall can be permitted by OMS network system administrators. A record of rules explaining why certain inbound traffic has been allowed through the firewall is kept and these rules will be regularly reviewed to ensure they are current and accurate.
- * Anti-malware and anti-virus scanning will be implemented across the OMS domain. The Smoothwall filter will screen out some potentially harmful traffic and inbuilt anti-malware and anti-virus software in both Google and Microsoft will further



screen data. Reviews as to whether additional anti-malware/anti-virus software is required will be undertaken.

ACCOUNT SECURITY

* School email addresses are all held within the OMS network domain. Staff emails are all two step verified, student emails are single factor verified, administrator and cross system users are multi factor verified.

* Successful cyber attacks target user accounts with the widest access and highest privileges on a network. At OMS this is the Admin account. OMS will limit the number of people able to access the Admin account and ensure Multi Factor Authentication is enabled. Users should have a separate account for routine business, including internet access, if their main account:

- is an administrative account
- enables the execution of software that makes significant system or security changes
- can make changes to the operating system
- can create new accounts
- can change the privileges of existing accounts

* All unused email addresses or accounts will be removed two months after a pupil has left OMS or one month after an employee has ended their employment. Where necessary the Google Documents, Spreadsheets and Forms belonging to staff email addresses/drives will have their ownership transferred to new members of staff or supervisory staff.

* Authentication will be required to access any sensitive school data. Both the Engage information system and Google Workspace for Education require two step verification to log in and access personal information.

* High function, systems administration or multi level privilege accounts will be protected by multi factor authentication.

* Accounts should have the access they require to perform their role and should be authenticated to access data and services. Administrator privileges are restricted within Google Workspace at OMS and these accounts should be protected by multi factor authentication.

PASSWORDS

* Password protocols require medium to strong passwords with a minimum of 8 characters, combined with two step verification. OMS uses a deny list through the Smoothwall Filter and Firewall system.

* Protection against brute force attack of incorrect passwords being used repeatedly is under review as of September 2025. It is likely that OMS will implement a 10 attempt lock out on devices. Once this security protocol is agreed (pending audit of all network devices) then this policy will be updated. OMS is using NCSC guidance on password and device security as the basis of its review [Here](#)



* Any compromised passwords or passwords that are suspected to be compromised will be changed immediately.

RESPONSIBILITY FOR DIGITAL SAFEGUARDING

OMS has designated the following posts/individuals to be responsible for ensuring the standards for digital safeguarding at school are being met:

DSL - Katie Townsend (Principal and SLT)

DDSL - Olivia Packe (SENDSCO and SLT)

DSL with responsibility for Digital Safeguarding Teresa Andrews (School Business Manager)

The staff listed above will be responsible for:

- procuring filtering and monitoring systems and reviewing this annually
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision and carrying out checks
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Filtering and monitoring systems will be reviewed immediately if a safeguarding risk is identified, there is a change in working practices or new technology is introduced. Otherwise it will be reviewed at least annually.

OMS will keep a log of the filtering and monitoring system checks and will record:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions
- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- blocklists are reviewed and they can be modified in line with changes to safeguarding risks

We will use South West Grid for Learning's (SWGfL) [testing tool](#) to check our filtering system is blocking access to:

- illegal child sexual abuse material
- unlawful terrorist content
- adult content



This policy was approved by the School Principal – Katie Townsend - on 08/09/2025

The implementation of this policy will be monitored by the: School Business Manager – Teresa Andrews.

The *Designated Safeguarding Lead* (School) is: Katie Townsend.

Serious online safety incidents must be reported to:

Operational Director, Blenheim Schools – Gemma Mann.

IT security concerns must be reported to security@ofgl.co.uk

A serious data breach or cyber attack must be reported to the National Fraud and Cyber Crime Centre, ACTION FRAUD, on 0300 123 2040, there is a link [HERE](#) . A serious cyber breach can involve loss of personal or sensitive data, unauthorised access to systems, copying, tampering or damaging information etc.

Where applicable schools should also report cyber attacks to the ICO – Information Commissioners Office and the link is [Here](#).

Local Authority Safeguarding Officer/DOfA or equivalent/agency safeguarding concerns are reported to:

- Director of Safeguarding/Safeguarding Adviser (safeguarding@ofgl.co.uk)
- Operational Director
- Police



Appendix A School Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within and beyond their school lives. The internet and other digital information and communications technologies are powerful tools, which open 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 team members to be more creative and productive in their work. All users should always be entitled to safe internet access and the acceptable use agreement will support this.

I understand that I must use the school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I agree to follow the rules below when using ICT at Oxford Montessori Schools

- I will only use IT at school for school purposes as directed by my teacher. I will not use school devices for online gaming, online gambling or internet shopping and I will not visit sites that I know or suspect to be unsuitable.
- I will log in to IT systems using my own username and password only. I will not share my username or password with anyone else nor will I try to use another pupil's or team member's username and password.
- I will not let anyone else use a device I am logged into with my username and password, this includes other pupils and siblings.
- I will ask permission before using a memory stick or other storage device (including phones and tablets) on a school computer.
- I will only open and delete my own files.
- I will never give out my own or other people's name, address (including email) or phone number online.
- I will never upload any images of school activities to any social networking site.
- I will not deliberately look for, save or send anything that could be perceived to be obscene, hateful, threatening or offensive.
- I will not install, attempt to install or store programmes or software on any school device, nor try to alter the computer settings.
- I will not try to download or use any programs or software that might allow me to bypass the School's IT filtering systems that are in place to prevent access to inappropriate or illegal content.
- I understand that sending a message with the deliberate intention of making another person feel offended, embarrassed, threatened or hurt is bullying, and will be dealt with according to the school Anti-bullying policy.
- If I see anything I am unhappy with on the computers or other devices, I will turn the screen off and tell a team member, my parent/carers or other appropriate adult straight away.
- I understand that the school can check my computer or other devices and that my parents/carers can be contacted if the school is concerned about my e-safety.

- I understand that I am responsible for my own behaviour and actions when using technology or the internet.
- I understand that the sanctions for misuse of ICT will be in line with the School's Behaviour Policy and may include serious sanctions for actions such as bullying or possessing or sending offensive material.



Remote Learning

- I will only use technology for school purposes as directed by my teachers.
- I will only browse, download, upload, or forward material that is related to my learning as directed by my teachers. If I come across material that may be considered offensive or illegal (accidentally or otherwise) I will report it immediately to my teacher or a parent/carer.
- I will make sure my communication with students and teachers is responsible and sensible. I will only use language and make comments that are supportive of my learning and the learning and wellbeing of others.
- I will maintain the same behavioural standards as would be expected in a real classroom for example, not interrupting the teacher, writing on the whiteboard or chatting with other pupils
- I will never record (video and/or audio) or take photos of my classmates or teachers during any online interaction using either my phone or any other device or computer.
- I understand that my use of applications provided by the school will be monitored and logged and can be made available to my teachers.

Pupil Name:		
School Leader Signed:		Date:
Parent/Carer Signed:		Date:



School Adapted Acceptable Use Agreement

At school we use computers, and other resources connected to the internet and our wireless network. These rules will keep us safe and help us to be fair to others.

- I will keep my passwords for login into any computer or application to myself – if I think others know my passwords, I will tell my teacher.
- I shall use the online activities and sites which school allows me to access from home appropriately.
- I will not bring in memory sticks into school unless I have been given permission.
- I will not use my own mobile device/ phone in school unless I am given permission from my teacher.
- If the computer asks for an update, I shall check this with my teacher.
- I will only use the computer for things my teacher has told me to.
- I will not use the internet to access unsuitable material.
- The messages I send will be polite and respectful.
- I will always report anything that I feel is unkind or makes me feel unsafe or uncomfortable to my teacher. I will not reply to any nasty messages.
- In school, I will only use my school e-mail and only e-mail people my teacher has approved.
- I will always keep my personal details private (e.g., my name, mobile phone number, family information, journey to school, pets, hobbies).
- I will not register my details with online activities and websites without the permission of my teacher.
- I will not share files or photos without the permission of my teacher.
- I will not copy text or pictures from the internet and pretend it is my own work.
- I understand that the school will check my computer files and will monitor the Internet sites I visit.
- I will treat computer equipment, like all school equipment, with care and respect.
- I know that if I break the rules, I might not be allowed to use a computer.

Pupil Name:		
School Leader Signed:		Date:
Parent/Carer Signed:		Date:



Child -friendly Acceptable User Agreement Statements

The following statements can be copied and pasted to your own document or can be used as prompts for discussion.

If appropriate, include a 'signing' section at the bottom.



 My name is:




 My trusted adults are:





 I will ask for help






 I will ask to use a computer






 I will ask to use an ipad






 I will ask to use a phone






 I will ask to use the internet













 I will tell a trusted adult if i see something that





 makes me scared.











 I will tell a trusted adult if i see something that





 makes me worried.











 I will tell a trusted adult if i see something that





 makes me sad.











 If i don't like something i see, i will tell my




 trusted adult.





BLENHEIM
SCHOOLS