Rumney
Primary School

Nurture the Child, Nurture the Leaner

Online Safety Policy

Headteacher: Mrs Eleri Williams

Chair of Governors: Mr David Baker

The United Nations Convention on the Rights of the Child (CRC) is at the heart of our school's planning, policies, practice and ethos. As a rights respecting school we not only teach about children's rights but also model rights and respect in all relationships. This policy is linked to:

Article 3: ***Everyone who works with children should always do what's best for each child;***
Article 13: Your right to have information;
Article 16: Your right to have privacy;
Article 17: Your right to honest information that you can understand;
Article 19: You should not be harmed and should be looked after and kept safe;
Article 34: You should be protected from sexual abuse;
Article 36: You should be protected from doing things that could harm you.

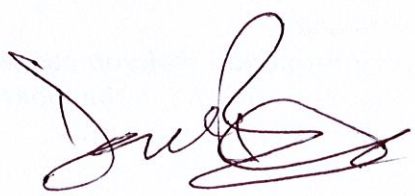
DEVELOPMENT, MONITORING & REVIEW OF THIS POLICY

This Online Safety Policy has been developed by a working group made up of:

- Headteacher
- Online Safety co-ordinators (Mike Carne)
- ICT co-ordinator (Mike Carne)
- DCF co-ordinators (Rachel Howells & Mike Carne)
- Staff
- Governors

SCHEDULE FOR DEVELOPMENT, MONITORING & REVIEW

This policy was agreed by teachers:	September 2023
This policy was agreed and adopted by the Governing Body:	September 2023
The implementation of this Online Safety Policy will be monitored by the:	ICT co-ordinator: Mike Carne DCF co-ordinator: Rachel Howells Online Safety co-ordinator: Mike Carne Headteacher
Monitoring will take place at regular intervals:	Annually, or as required in the light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.
The *Governing Body/governors subcommittee* will receive a report of the implementation of the online safety policy generated by the monitoring groups (which will include anonymous details of online safety incidents) at regular intervals.	Annually or when necessary
The online safety policy will be review annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to online safety or incidents that have taken place. The next review date will be:	September 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed.	Schools ICT Services, Cardiff LA, iTeach, Police, Child Exploitation and Online Protection Centre.
Chair of Governors' Signature	



10 X 2023

Scope of the Policy

This policy applies to all members of the school (including staff, pupils, volunteers, parents, carers, visitors, community users) who have access to, and are users of school ICT systems, both in and out of the school. The Education & Inspection Act 2006 empowers Head teachers to such extent as it reasonable, to regulate 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 safety incidents covered by this policy, which may take place outside of school, but is linked to membership of the school for example, though not limited to, WhatsApp, Facebook, TikTok, Instagram, Snapchat and any forms of social media. The Education Act 2011 increased these powers with regard to the searching for and of, electronic devices and the deletion of data. In case of both Acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy, and associated 'Behaviour' and 'Anti Bullying' policies, and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour if it takes place in school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body who will receive regular information about online safety incidents and monitoring reports. Mr David Baker has been appointed as the online safety governor. The role of online safety governor includes:

- Regular meetings with the online safety co-ordinator.
- Regular monitoring of online safety incident logs.
- Regular monitoring of filtering/change control logs.
- Reporting to relevant Governors' meetings.

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinators.
- The Headteacher and (at least) one other member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents – included in a later section – 'Responding to Incidents of Misuse' and relevant Local Authority HR/other relevant body disciplinary procedures).
- The Headteacher is responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This

is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Headteacher will receive regular monitoring reports from the Online Safety Co-ordinator.

The Online Safety Co-ordinator Role

The Online Safety Co-ordinator is responsible for:

- Leading the online safety group (a group made up from the wider school community: Online Safety Co-ordinator [Mike Carne], Online Safety Governor [David Baker] and a parent representative [NAME]).
- Taking day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies, the online safety section on the school website and documents.
- Ensuring all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Providing training and advice for staff.
- Liaising with the Local Authority and relevant bodies.
- Liaising with iTeach technical staff.
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments.
- Meeting regularly (every term or when required) with Online Safety Governor to discuss current issues, review incident logs and if possible, filtering change control logs.
- Attending relevant meetings of Governors.
- Reporting regularly to the Headteacher and Senior Leadership Team.

Technical Staff (iTeach)

Technical staff are responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse of malicious attack.
- The school meets the required online safety technical requirements as identified by the Local Authority or other relevant body and also the online safety policy/guidance that may apply.
- Users may only access the networks and devices through properly enforced password protection policy, in which passwords are regularly changed.
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of the network/internet/learning platform/Hwb/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Online Safety Co-ordinator/officer for investigation/action/sanction.
- That the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

Teaching and Support Staff (and volunteers)

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, understood and signed the staff Acceptable Use Agreement and the Mobile Device Acceptable Use Policy, both found within the Appendix.
- They report any suspected misuse or problem to the Headteacher/Online Safety Co-ordinator for investigation/action/sanction.
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems (except for in extreme/emergency situations).
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the online safety and acceptable use agreements.
- 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 regards to these devices.
- In lessons where internet use is pre-planned learners should be guided to site 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 Child Protection Teacher

The designated senior person should be trained in online safety issues and be aware of potential for serious safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Online Safety Group

The Online Safety Group is a consultative group that has a wide representation from the school community (teacher responsible for Online Safety, Online Safety Governor and a parent representative), with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Co-ordinator/officer with:

- The production/review/monitoring of the school Online Safety Policy/documents.
- The production/review/monitoring of the school/filtering policy (and requests for filtering changes).

- Mapping and reviewing the online safety curricular provision – ensuring relevant breadth and progression.
- Monitoring network/internet/incident log where possible.
- Consulting stakeholders – including parents/carers and the learners about the online safety provision.
- Monitoring improvement actions identified through use of 360 degree safe Cymru self-review tool.
- Children group from Digital Leaders.

Pupils

All pupils:

- Are responsible for using the school digital technology systems in accordance with the learner Acceptable Use Agreement.
- 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. 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 safety practice when using digital technologies out of school and realise that the school's Online Safety 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/carers understand these issues through parents' evening, newsletters, letters, website, Hwb learning, platform and information about national or local online safety campaigns/literature. Parents/carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' section of the website, Hwb, learning platform and online learner records.

Community Users (e.g. Midday Supervisors, Supply Teachers, Parent Helpers etc.)

Community users who access school systems/website/Hwb/learning platform as part of the wider school provision will be expected to sign a community user AUA (Appendix D) being provided with access to school systems.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and build up their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum across a range of subjects, (e.g. ICT/Health and Wellbeing/DCF) and topic areas and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and circle time activities.
- Internet Safety week should be celebrated by all classes each year with an assembly to share learnings and follow up activities should be planned to ensure the annual message is reinforced.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be given opportunities, where appropriate, to fulfil the Digital Competency Framework (DCF) alongside and throughout their learning.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. N.B. Additional duties for the school under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Pupils should be helped to understand the need for the Learner Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Digital Leaders will support pupils in the class in understanding the importance of online safety.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices in accordance with the Acceptable Use Agreement.
- In lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- It is acceptable that from time to time, for good educational reasons, older pupils may need to research topics (e.g. racism, discrimination) that would normally result in internet searches being blocked. In such situation, staff can request that the technical staff (or other nominated 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 or that.

Education – Parents/Carers

Many parents/carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents/carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities.
- Letters, newsletters, website, learning platform Hwb.
- Workshops for parents/carers.
- High profile events/campaigns, e.g. Safer Internet Day.
- Reference to the relevant websites/publications on school newsletters, e.g. https://hwb.wales.gov.uk/ www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – the Wider Community

The school will provide opportunities for the local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide safety information for the wider community.

Education and Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Co-ordinator will receive regular updates through attendance at external training events, (e.g. from Consortium,/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.

- The Online Safety Co-ordinator will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisations (e.g. SWGfL).
- Participation in school training/information sessions for staff and parents.

Technical – infrastructure/equipment, filtering and monitoring

The school has a managed ICT service provided by the LA and iTeach, however, it is the responsibility of the school to ensure that they carry out all the online safety measures that would otherwise be the responsibility of the school. It is also important that iTeach technicians are fully aware of the school Online Safety Policy and Acceptable Use Agreement.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the ICT Co-ordinator who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their passwords art regular intervals.
- The "master/administrator" passwords for the school digital systems, used by the network manager (or other person) must also be available to the Headteacher and kept in a secure place within the school.
- The ICT Co-ordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs). Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider (LA) by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. The Headteacher and Online Safety Co-ordinator use SWURL to

list any inappropriate websites, which break through the filter. There is a clear process in place to deal with requests for filtering changes.

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Where possible, technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- If an Online Safety incident occurs, all staff members know that it must be reported to the Online Safety Co-ordinator immediately for investigation, a log must be recorded in the appropriate way and a record of the incident should be uploaded to the electronic safeguarding system My Concerns. The Online Safety Co-ordinator will follow the appropriate steps listed in the Online Safety Incident Flowchart (on page 22) and the necessary actions/sanctions will be carried out. The Headteacher will always be informed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstation, 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.
- The Community User Acceptable Use Policy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Staff and Community Users Acceptable Use Policies are in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school/college.
- A Staff Acceptable Use Policy is in place that outlines permission to download executable files and install programmes on school devices.
- A Staff Acceptable Use Policy is in place regarding the use of removeable media (e.g. USB memory sticks) by users on school devices. Files where personal information is recorded, e.g. school reports, assessment trackers, ALN reports and information should not be stored on a USB memory drive, instead this information should be stored in the shared Google Drive. Personal data cannot be taken off the school site unless specific information is granted and appropriate measures are put in place. Any information that is shared via email, but be done so via staff secure school Google email accounts.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop/chromebook or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud based services such as email and data storage.

All users should understand the primary purpose of the use of mobile/personal devices at school is educational. Pupils are not permitted to use personal devices on site and are provided with the equipment that they need. All staff use school issued devices during classroom activities. Staff may only photograph pupils where parental / guardian permission

is given; school devices must be used. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and 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 harm.

When using digital images, staff should inform and educate learners 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 in 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 learners in the digital/video images, or include the names of staff or pupils.
- 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 / videos should only be taken on school equipment.
- Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or X (formally known as Twitter), particularly in association with photographs, nor will locations be mentioned (unless posting AFTER an activity has taken place) e.g. posts for educational visits will only be uploaded after pupils return. The only exception to this is when pupils are on a residential trip however their location will not be revealed, e.g. It is fine to post 'Year 6 enjoying themselves on their residential trip' NOT 'Year 6 enjoying themselves at Abernant.'
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website/X account. Children without written permission must not be included in photographs that would potentially be posted on the website/X account.
- Pupils' work can only be published with the permission of the pupils and parents/carers.

Data Protection

Personal data will be recorded, process, transferred and made available according to the Data Protection Act 2018. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines. General Data Protection Regulation (GDPR) establishes six enforceable principles that must be adhered to at all times in that information must be:

- Processed fairly, lawfully and in a transparent manner
- Collected for specified explicit and legitimate purposes and not further processed in a manner that is incompatible for those purposes.
- Adequate relevant and limited to what is necessary in relation to the purpose for which it is processed
- Accurate and where necessary kept up to date
- Kept in a form that permits identification of data subjects for no longer than necessary for purposes that which the personal data is processed
- Processed in a manner that ensures appropriate security of the personal data.

The School is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected.
- Inform individuals when their information is shared, and why and with whom it was shared.
- Check the quality and the accuracy of the information it holds.
- Ensure that information is not retained for longer than is necessary.
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Share information with others only when it is legally appropriate to do so.
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Right of Access, right of rectification, right to erasure, right to restrict processing, right to data portability and right to object.
- Ensure our staff are aware of and understand our policies and procedures.
- Ensure our staff are provided with adequate training and support.

The school must be aware that Under the Data Protection Act 2018, parents/carers/pupils have the right to find out what information the school/college stores about them. These include the right to:

- Be informed about how data is being used.
- Access personal data.
- Have incorrect data updated.
- Have data erased.
- Stop or restrict the processing of data.
- Data portability (allowing the school/college to get and reuse data for different services).
- Object to how data is processed in certain circumstances.

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.**
- 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 / systems.

Personal data should not be stored on any portable computer system, memory stick or any other removable media.

Communications

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

Communication Technologies	Staff & other adults				Learners			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓*
Use of mobile phones in lessons			✓**					✓
Use of mobile phones in social time (away from pupils)	✓							✓
Taking photos on mobile phones			✓					✓
Use of other mobile devices e.g. tablets, gaming 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				✓			✓	

*Mobile phones permitted in exceptional circumstances with prior agreement from the Headteacher, e.g. where pupils walk to or from school, however are not used for educational purposes. This applies to Year 6 pupils only. See policy for further details.

**Specific staff will be permitted to have mobile phones where there are health care or wellbeing needs around pupils. This is with the agreement of the Headteacher.

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

- Staff and pupils should use only the school email service to communicate with others when in school, or on school systems, (e.g. by remote access).
- Users must immediately report to the Online Safety Co-ordinator 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, learning platform, etc.) must be professional in tone and content. Phone calls with parents / carers are encouraged rather than emailing.** These communications may only take place using official (monitored) school system Teacher to Parent text system or teacher emails (and the Deputy Headteacher should be bcc'd in). Personal email addresses, text messaging or social media must not be used for these communications. The Deputy Headteacher MUST be bcc'd into any communication emails between parents / carers and staff.
- Google Class/Hwb private message to parents regarding homework/online learning must always be related to the work and professional in tone. The school's marking policy should be used.
- Whole class/group email addresses may be used in Reception to Year 2 (although they have their own addresses via the Hwb learning platform and Google), while pupils in Year 3 to Year 6 will use their Google email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risk 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.
- 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

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for learners and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm through:

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:

- A process for approval by senior leaders.
- Clear processes for the administration and monitoring of these accounts — involving at least two members of staff.
- A code of behaviour for users of the accounts
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- School use of social media for professional purposes will be checked regularly by the Headteacher, Online Safety Co-ordinator and Online Safety Group to ensure compliance with the social media, data protection, communications, digital image and video policies.

Unsuitable/inappropriate activities:

Some internet activity, e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities, e.g. online bullying is also banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but are inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in, or out of, school when using school equipment or systems. The school policy restricts usage as follows:

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.					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008.					✓
	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.					✓
	Pornography.				✓	
	Promotion of any kind of discrimination.				✓	
	Threatening behaviour, including promotion of physical violence or mental harm.				✓	
	Promotion of extremism or terrorism.				✓	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school/college or brings the school/college into disrepute.				✓	
Using school systems to run a private business.					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.					✓	
Infringing copyright.					✓	
Revealing or publicising confidential or proprietary information, (e.g. financial/personal information, databases, computer/network access codes and passwords).					✓	
Creating or propagating computer viruses or other harmful files.					✓	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet).					✓	
Online gaming (educational).		✓				
Online gaming (non-educational).					✓	
Online gambling.					✓	
Online shopping/commerce.			✓*			
File sharing.		✓				
Use of social media (educational/school related).		✓				
Use of social media (private accounts).					✓	
Use of messaging apps (school account)			✓**			
Use of messaging apps (private accounts).					✓	
Use of video broadcasting, e.g. YouTube			✓			

*Using online shopping sites on school equipment may only be conducted by the Headteacher or Office Administrator for school equipment only. No other staff are permitted to use school equipment for such purposes.

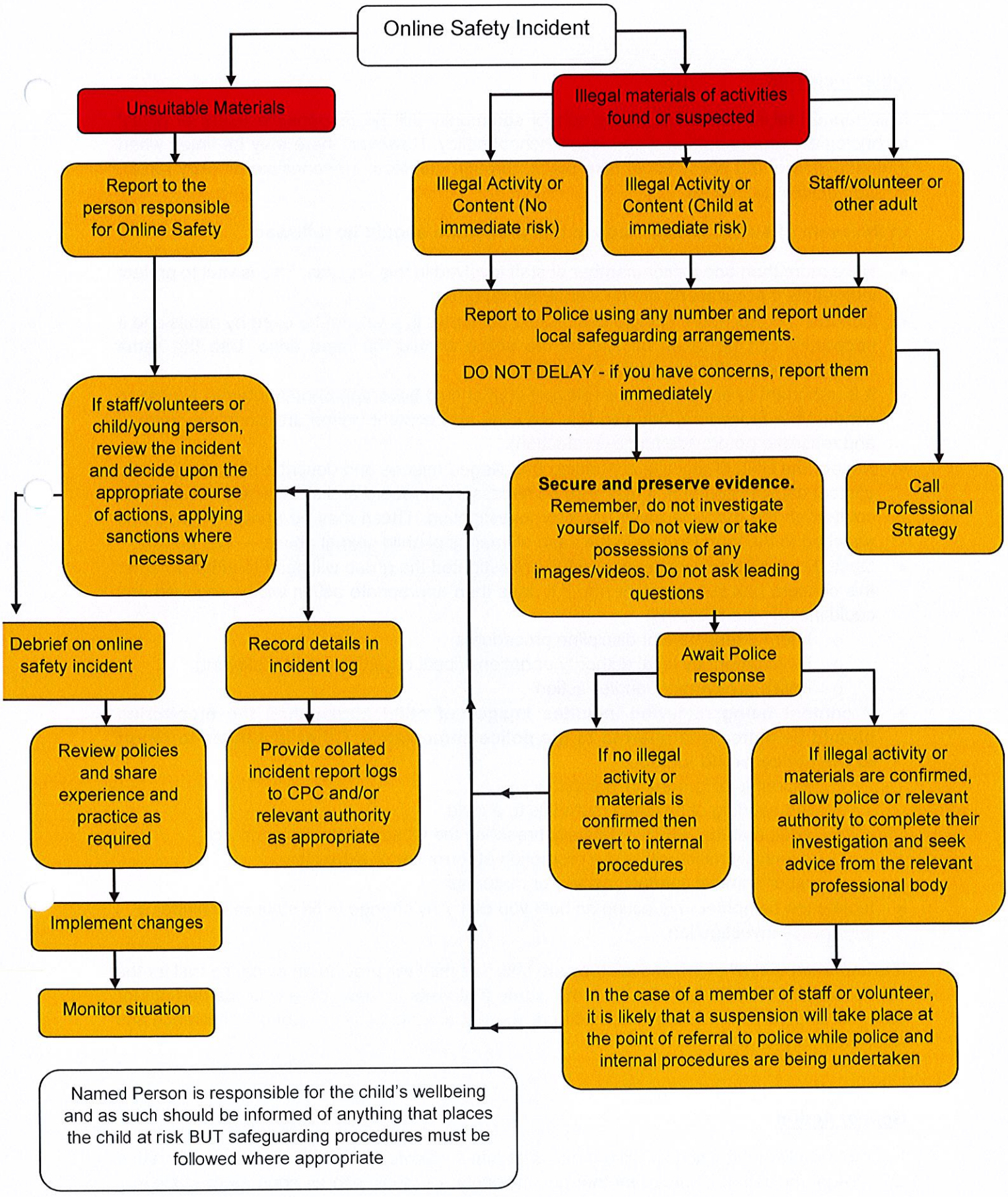
**School messaging apps cannot be used during lesson time and must always be used away from pupils.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the flowchart (below and appendix) for responding to Online Safety Incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials of activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/volunteer or other adult
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY - if you have concerns, report them immediately
If staff/volunteers or child/young person, review the incident and decide upon the appropriate course of actions, applying sanctions where necessary
Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possessions of any images/videos. Do not ask leading questions
Call Professional Strategy
Debrief on online safety incident
Record details in incident log
Await Police response
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
If no illegal activity or materials is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT safeguarding procedures must be followed where appropriate

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- 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 designated 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 procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of 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, signed and attached to the form (except in the case of images of child sexual abuse — see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures.
    - Involvement by local authority or national/local organisation (as relevant).
    - Police involvement and/or action
- **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 o promotion of terrorism or extremism
    - 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Action

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Learner Actions

Incidents	Refer to class teacher	Refer to Deputy Headteacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanctions e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		✓	✓	✓					
Unauthorised use of non-educational sites during lessons.	✓	✓	✓			✓		✓	
Unauthorised use of mobile phone/ camera/other mobile devices.	✓	✓	✓			✓		✓	
Unauthorised use of social media/messaging apps/personal email.	✓	✓	✓			✓		✓	
Unauthorised downloading or uploading of files.	✓	✓	✓		✓	✓		✓	
Allowing others to access school network, by sharing username and passwords.	✓	✓	✓		✓	✓		✓	
Attempting to access or accessing the school network, using another pupil's account.	✓	✓	✓		✓	✓			✓
Attempting to access or accessing the school network, using the account of a member of staff.	✓	✓	✓		✓	✓			✓
Corrupting or destroying the data of other users.	✓	✓	✓			✓	✓		✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.	✓	✓	✓			✓	✓	✓	✓
Continued infringement of the above, following previous warnings or sanctions.	✓	✓	✓			✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.			✓			✓	✓	✓	✓
Using proxy sites of other means to subvert the school's filtering system.			✓		✓	✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident.			✓		✓	✓	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material.			✓	✓		✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.			✓	✓		✓	✓	✓	✓

Staff Actions

Incidents	Refer to Online Safety Co-ordinator	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to technical support staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		✓	✓	✓	✓		✓	✓
Inappropriate personal use of the internet/social media/personal email.	✓	✓	✓		✓	✓		✓
Unauthorised downloading or uploading of files.	✓	✓	✓		✓	✓		✓
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.	✓	✓				✓		✓
Careless use of personal data, e.g. holding or transferring data in an insecure manner.	✓	✓	✓			✓		✓
Deliberate actions to breach data protection or network security rules.	✓	✓	✓			✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.	✓	✓	✓	✓	✓	✓	✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.	✓	✓	✓				✓	✓
Using personal email/social networking/messaging to carrying out digital communications with learners.	✓	✓	✓	✓	✓	✓	✓	✓
Actions which could compromise the staff member's professional standing.	✓	✓	✓			✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.	✓	✓	✓			✓	✓	
Using proxy sites or other means to subvert the school's filtering system.	✓	✓	✓	✓	✓	✓	✓	✓
Accidentally accessing offensive pornographic material and failing to report the incident.	✓	✓	✓			✓		✓
Deliberately accessing or trying to access offensive pornographic material.	✓	✓	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations.	✓	✓				✓		✓
Continued infringement of the above, following previous warnings or sanctions.	✓	✓	✓		✓	✓	✓	✓

Equality Impact Statement

At Rumney Primary School, we recognise and celebrate the fact that British and Welsh society is made up of people from diverse backgrounds and life experiences and as such, seek to reflect this in all of our school policies. In accordance with the Equalities

Act 2010 our policies and learning and teaching strategies fulfil the duties to promote equality for people with protected characteristics, and embed fairness and equality at the heart of our school community and in all aspects of our school plans and policies. Through this policy we seek to:

1. Eliminate discrimination, harassment and victimisation.
2. Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
3. Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

At our school, we aim to provide a happy, caring environment in which all children can feel confident and able to learn. We seek to foster an environment of mutual respect and support between all staff, pupils, parents and carers and the wider community and this is reflected in the content of each policy.
The school values and encourages involvement of people from all sections of the local community and through this involvement aims to provide positive images, role models and opportunities that challenge stereotyped thinking.

Appendix

- Pupil acceptable use agreement – Reception, Year 1, Year 2
- Pupil acceptable use agreement – Year 3 to Year 6
- Parent / Carer acceptable use agreement
- Consent forms for Photographic images
- Staff and Volunteer acceptable use policy and agreement
- Mobile Technologies Policy
- Reporting Log
- Links to other organisations

Rumney Primary School

Pupil acceptable use agreement – Reception, Year 1, Year 2

This is how we stay safe when we use iPads and Chromebooks:

- ✓ I will ask a teacher or another adult from the school if I want to use the iPads or Chromebooks.
- ✓ I will only use activities that a teacher or another adult from the school has told or allowed me to use.
- ✓ I will take care of the computers and other equipment.
- ✓ I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.
- ✓ I will tell a teacher or another adult from the school if I see something that upsets me on the screen and switch off the device.
- ✓ I know that if I break the rules I might not be allowed to use an iPad or Chromebook.

Signed (child): .....

Year group: .....

Date: .....

Rumney Primary School

Acceptable Use Agreement – Year 3 – Year 6

I understand that I whilst I am a member of Rumney Primary School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology and digital communication will be supervised and monitored.
- I will keep my username and password safe and secure and will not share it with anyone, neither will I use anyone else'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 be aware of "stranger danger" when I am communicating online.
- I will not share my personal information or information about others when online (this could include names, addresses, e-mail addresses, telephone numbers, age gender, school details).
- I will not arrange to meet people off-line that I have communicated with online. If someone asks to meet with me, I will inform a trusted adult.
- I will immediately tell a trusted adult if anything makes me feel unconformable or upset when I see it online. I will also switch the screen off immediately.

For the safety of others:

- I will respect the way that others use their technology and not access, copy or change their work without their permission.
- I will be polite and responsible when I communicate with others.
- I will not take or share images of anyone without their permission and never identify individuals.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- If I bring my mobile phone to school it will be stored away for the duration of the school day and never used during the school day.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible adult if I find damage or fault with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devises belonging to the school.
- I will only open hyperlinks in emails or attachments to emails, if I know and trust the person who sent the email, and have no concerns about the validity of the email.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the school and where they involve my membership of our school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to follow this acceptable use agreement, there may be serious consequences for my behaviour, this could include loss of access to the school network/internet, parents/carers contacted and in the event of illegal activities, this could include the involvement of the police.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines.

Name of learner: .....

Signature: .....

Year group: .....

Date: .....

Rumney Primary School

Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.
This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents / carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will endeavour to ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Learner Acceptable Use agreement is available on the school website, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents/carers are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

As the parent/carer of the pupil/s named below, I give permission for my son(s)/daughter(s) to have access to the internet and to digital technology systems at school.

I understand that the school has discussed the acceptable use agreement with my son(s)/daughter(s) and that he/she has signed the agreement. I also understand that that they will receive on-going 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 applying monitoring and filtering systems, to ensure that pupils will be safe when they use the internet and digital technology 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 child's activity on the digital technology systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

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.

Name of pupil(s): .....

Signed: ..... Date: .....

NB: In accordance to data collection procedures, please note that this information will stored securely and only be accessed by staff who are authorised by the Headteacher to do so. The form will be kept for as long as your child attends Rumney Primary School, after which time the form will be shredded. Should you sign the form on behalf of two or more children, the form will be kept until the youngest child leaves the school.

Rumney Primary School

Use of Digital/Video Images

The use of digital / video images plays an important part in learning activities. Learners and members of staff may use cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons and may also be used to celebrate success through their publication in newsletters, on the school website, social media platforms and very occasionally in the public media.

The school will comply with GDPR and request parents / carers permission before taking images of their child. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

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. To respect everyone's privacy and protection, these images **must not** be published / made publicly available on any social networking sites.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children.

Digital/Video Images Permission Form

Parent / Carer Name: .....

Pupil's Name: .....

*Please tick each of the following statements where **consent is given**:*

I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school. ☐

I agree that if I take a digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images. ☐

The school may use my child's photo for a publicity shot in a local or national paper where first names may be used (Individual/or group photo). ☐

The school may use an **individual** photograph of my child for the school's website / twitter page. Names will not be used. ☐

The school may use a **group** photo of my child for the school website / twitter page. Names will not be used. ☐

Signed: ..... Date: .....

Rumney Primary School

Staff and Volunteers Acceptable Use Policy and Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools 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 access to the internet and digital technologies 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 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 technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities 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 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 recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the children and young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, e-mail, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of the school.
- I understand that the school digital technology systems are intended for educational use and that I will only use the school systems for such purposes.
- 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 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, on the school's X account) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner. The Deputy Headteacher will be Bcc'd into all communications with parents / carers which can only occur during the hours stipulated in the school's policy.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- When I use my personal mobile devices 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 may access work emails on my personal mobile device, providing that access is password protected.
- I may not access the school's Google drive on my personal device.
- I will not use personal e-mail addresses on the school ICT systems without the permission of the Headteacher.
- I will not open any hyperlinks in e-mails or any attachments to e-mails, unless the source is known and trusted, or if I have any concerns about the validity of the e-mail (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that data is kept on the school's shared drives and not on any portable devices, e.g. external USB memory device.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist 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.
- 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 documents containing personal data must be held in lockable storage.
- Should I access any pupil data on a school device when I am off site e.g. pupil target plans, I must ensure that I use a secure network and that such data is logged out of correctly. I must ensure that whilst accessing such documents that the device is not left unattended.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

- I will ensure that I have permission to use the original work of others in my own work
- where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in the school, but also applies to my use of school 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 agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the local authority and in the event of illegal activities the involvement of the police.

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

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Rumney Primary School

Mobile Technologies Policy

Mobile technology devices may be a school owned/provided or privately-owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

The absolute key to considering the use of mobile technologies is that the learners, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, acceptable use agreements and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Pupils now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen pupils learning, but they can also develop digital resilience, fluency and citizenship in learners that will prepare them for the high-tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all learners, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

Rumney Primary School provides all teaching staff (and non-teaching staff as required), their own laptop device (ThinkPad) or Chromebook; these can used on and off site for school work only. Each class also has a 'teacher' iPad. All other technologies needed for teaching and learning, e.g. beebots, green screen, are also provided by the school. There is therefore no requirement for staff to bring other personal devices to school for educational purposes.

It is recognised however that staff may wish to bring their personal mobile phone devices to school. This is permitted, however should be stored away from pupils during the school day. Staff are permitted to access their work email from their personal devices, provided that this is password protected. It is the responsibility of the member of staff to ensure their device is virus protected. Access to the school's Google Drive is not permitted on personal devises.

The school operate a WhatsApp group, to quickly communicate with staff, however this should not be accessed within learning time and should only be used during break and lunch times. Mobile devices should be kept away from pupils. Specific permission needs to be sought directly from the Headteacher or Deputy Headteacher should a staff member need access to their mobile device at a particular time during the day; this should be for emergency use only.

The school allows:

	School devices			Personal devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[1]	Learner owned	Staff owned	Visitor owned
Allowed in the school	Yes	Yes	No	Yes[2]	Yes[2]	Yes[2]
Full network access	*Yes*	*Yes*	No			
Internet only			No		Yes	Yes
No network access			No	No		

- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- When a device is no longer in use by the school, this will be managed by the school IT management provider, i-Teach.
- All school devices are subject to routine monitoring.
- *When personal devices are permitted:*
- Personal mobile phone devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers in agreement with the Headteacher).
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).

[1] Authorised device – only devices owned by the school should be used on site and therefore have access to the school's network system. The school does not facilitate a school / learner organised scheme.

[2] With the permission of the Headteacher, Year 6 pupils are permitted to bring a mobile phone to school should they be walking to or from school. This must be handed in at the start of the school day and locked away by the class teacher. This equipment is bought to school at the learner's own risk, no liability is taken by the school. Pupils are not permitted to use this device on school premises, any violation of this may result in the pupil not being able to bring their device to school. Staff are permitted to bring their personal mobile phone to school, however this should not be used during lesson time, only during recreational times and away from pupils. Individuals are responsible for storing these devises safely during the day. The school does not accept any liability for loss or damage. Training providers are permitted to bring their own devices to school. This is also at their own risk. They may access the internet whilst on promises.

- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security.
- The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues – these tasks should not be carried out on-site.
- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;
- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements.
- Users are responsible for keeping their school owned device up to date through software and security updates. The device is virus protected and should not be capable of passing on infections to the network. Any advice around this should be sought form the ICT co-ordinator.
- Users are responsible for charging their own school owned devices and for protecting and looking after their devices while in the school and if these are taken off-site.
- When the school google drive is accessed off site, care must be taken when accessing personal information, e.g. pupil trackers. When such information is on screen, devices should not be left unattended and care must be taken to close applications carefully after use of log out of the device correctly and securely.
- Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted at school.
- Personal devices must be in silent mode on the school site.
- School devices are provided to support learning.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc...) that would stop the device working as it was originally set up and intended to work is not permitted
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps.
- The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to learners on authorised devices once they leave the school roll.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately.
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions.

- Printing from personal devices will not be possible.

Insurance

The loss, damage or theft of any school owned devices must be reported to the Headteacher and reported to the Local Authority. Repairs or replacements may be covered by the school's insurance policy. Loss or damage to any personal devices that are brought in site are not covered in by the school.

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported by	Signature
			What?	By whom?		

Links to other organisations or documents

These may help those who are developing or reviewing an online safety policy.

UK Safer Internet Centre

- Safer Internet Centre
- South West Grid for Learning
- Childnet
- Professionals Online Safety Helpline
- Internet Watch Foundation

CEOP

- http://ceop.police.uk/
- ThinkUKnow

Others

- INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
- Netsmartz - http://www.netsmartz.org/index.aspx

Cyberbullying

- Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
- Scottish Government - Better relationships. better learning, better behaviour
- Welsh Government — Respecting Others
- Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
- Cyberbullying.org - http://www.cyberbullying.org/
- Enable — EU funded anti-bullying project - http://enable.eun.org/

Sexting

- UKCCIS - Sexting in schools and colleges: responding to incidents and safeguarding young people (to be added to both language versions)
- UKSIC — Responding to and managing sexting incidents

Social Networking

- Digizen — Social Networking
- SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
- Connectsafely Parents Guide to Facebook
- Facebook Guide for Educators

Curriculum

- SWGfL Online Safety Resource (accessed through Hwb)
- Alberta, Canada – digital_citizenship_policy_development_guide.pdf
- Teach Today — www.teachtoday.eu/
- Insafe - Education Resources

Mobile Devices/BYOD

Cloudleam Report Effective practice for schools moving to end locking and blockinq

NEN - Guidance Note – BYOD

Data Protection

- Information Commissioners Office:
  - Your rights to your information — Resources for Schools - ICO
  - ICO pages for young people
  - Guide to Data Protection Act - Information Commissioners Office
  - Guide to the Freedom of Information Act - Information Commissioners Office
  - ICO - Guidance we gave to schools/colleges - September 2012 (England)
  - ICO Guidance on Bring Your Own Device
  - ICO Guidance on Cloud Computing
  - Information Commissioners Office good practice note on takinq photos in schools/colleges
  - ICO Guidance Data Protection Practical Guide to IT Security
  - ICO - Think Privacy Toolkit
  - ICO — Personal Information Online — Code of Practice
  - ICO — Access Aware Toolkit
  - ICO Subject Access Code of Practice
  - ICO — Guidance on Data Security Breach Management
- SWGfL - Guidance for Schools/colleges on Cloud Hosted Services
- NEN - Guidance Note - Protecting School/college Data

Professional Standards/Staff Training

- Kent - Safer Practice with Technology
- Childne/TDA - Social Networking - a guide for trainee teachers & NQTs
- Childne/TDA - Teachers and Technology - a checklist for trainee teachers &
- NQTs
- UK Safer Internet Centre Professionals Online safety Helpline

Infrastructure/Technical Support

- Somerset - Questions for Technical Support
- NEN - Guidance Note - esecurity

Working with parents and carers

- Connect Safely - a Parents Guide to Facebook
- Vodafone Digital Parents Magazine Childnet Webpages for Parents & Carers
- Get Safe Online - resources for parents
- Teach Today - resources for parents workshops/education
- The Digital Universe of Your Children - animated videos for parents (Insafe)
- Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
  Insafe - A guide for parents - education and the new media
  Internetmatters.org