Mill Water School
admin@millwater.devon.sch.uk | www.millwater.devon.sch.uk | 01395 568890

Online Safety Policy and Agreements

Content

- Rationale
- Development, Monitoring and Review of the Online Safety Policy
- Schedule for Development, Monitoring and Review of the Online Safety Policy
- Scope of the Online Safety Policy
- Roles and Responsibilities
  - Governors
  - Headteacher and Senior Leaders
  - Online Safety Coordinator
  - ICT Technician
  - Teaching and Support Staff
  - Child Protection Officer / Designated Safeguarding Lead
  - Online Safety Working Group
  - Pupils
  - Parents / Carers
- Policy Statements
  - Education – Pupils
  - Education – Parents / Carers
  - Education – Extended Schools
  - Education and Training – Staff
  - Training – Governors
  - Technical – infrastructure / equipment, filtering and monitoring
  - Curriculum
  - Bring your own device (BYOD)
  - Use of digital and video images
  - Data Protection
  - Communications
  - Social Media – Protecting Professional Identity
  - Unsuitable / inappropriate activities
  - Responding to incidents of misuse
- Appendices
  - Mill Water School Filtering Policy
  - Mill Water School Password Security Policy
  - Mill Water School Personal Data Handling Policy
  - 14 Rules for responsible ICT use
  - Acceptable Use Policy for Pupils
  - Acceptable Use Policy for Parents / Carers
  - Acceptable Use Policy for Staff and Volunteers
  - Use of Digital Images – Photography and Video (includes consent form)

Rationale

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 and information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education, from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Online bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development, Monitoring and Review of the Online Safety Policy

This online safety policy has been developed by an online safety working group made up of:

- Online Safety Coordinator
- Senior Leadership Team
- ICT Technician
- School Business Manager

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development, Monitoring and Review of the Online Safety Policy

The Mill Water Online Safety Policy was approved by the Governing Body on:	July 2016
The implementation of this Online Safety Policy will be monitored by the:	Online Safety Working Group
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the Online Safety Working Group (which will include anonymous details of online safety incidents) at regular intervals:	Annually or as required
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	July 2017
Should serious online safety incidents take place, the following external persons/agencies should be informed:	CEOPS The Police

The school will monitor the impact of the policy using:

- Logs of reported incidents (via Safeguarding Termly Report to Governors)
- SWGfL (South West Grid for Learning) monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of Mill Water School Community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school IT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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 that take place out of school.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Teaching and Learning Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Coordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to Teaching and Learning Governors committee

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, although the day to day responsibility for online safety will be delegated to the Online Safety Coordinator.
- The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD (continuous professional development) to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that the ICT Technician/Business Manager implements a rolling programme of checking internet search history on each school computer. The Online Safety Coordinator and Headteacher will ensure the ICT Technician undertakes the appropriate training to facilitate this task.
- The Headteacher and the Online Safety Coordinator should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Online Safety Coordinator:

- leads the Online Safety Working Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT Technician
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments (held within Safeguarding Termly Report to Governors)
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- reports regularly to Senior Leadership Team

ICT Technician:

The ICT Technician is responsible for ensuring:

- that the school's IT infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority online safety policy and guidance.
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- that he keeps up to date with online safety technical information in order to effectively carry out his online safety role and to inform and update others as relevant.
- that the use of the network/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher (or Online Safety Governor for misuse by Head Teacher) for investigation.
- filtering sites identified as inappropriate.

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 school Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the Online Safety Co-ordinator or Headteacher for investigation.
- digital communications with pupils (email/voice) does not happen and should be reported if it occurs.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- pupils follow the school Online Safety and Acceptable Use Policy and understand it, where appropriate.
- they monitor IT activity in lessons, extra curricular and extended school activities.
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use.

Child Protection Officer / Designated Safeguarding Lead:

should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

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

Online Safety Working Group:

Members of the Online Safety Working Group are responsible for:

- the production/review/monitoring of the school Online Safety Policy/documents
- mapping and reviewing the online safety curricular provision
- the production/review/monitoring of the school filtering policy.

Pupils, where able:

- are responsible for using the school IT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. Where appropriate, parents/carers will sign on behalf of their child.
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on online 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of IT than their children. The school will therefore take every opportunity to help parents understand these issues through the Parents' Support Group, training, newsletters, letters, website and information about national/local online safety campaigns/literature.

Parents and carers will be expected 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
- Their children's personal devices in school

They will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy

Policy Statements

Education – pupils

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

Online safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of IT/PHSE/other lessons and should be regularly revisited – this will cover both the use of IT and new technologies in school and outside school.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
- Staff should act as good role models in their use of IT, the internet and mobile devices.

Education – parents / carers

Many parents and 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 on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

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

- Letters, newsletters, website
- Parents evenings, Parents' Support Group
- Reference to the ParentInfo website and the Digital Parenting Magazine (via School Website)

Education - Extended Schools

The school may offer family learning courses in IT, media literacy and online safety so that parents and children can together gain a better understanding of these issues. Messages to the public around online safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education and Training – Staff

It is essential that all staff receive online safety training and understand their 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. 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 Policies.
- The Online Safety Coordinator will receive regular updates through attendance at SWGfL/LA/other information/training sessions and by reviewing guidance documents released by BECTA/SWGfL/LA and others.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/training days.
- The Online Safety Coordinator will provide advice/guidance/training as required 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 subcommittee involved in IT/online safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/SWGfL or other relevant organisation.
- Participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

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 need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School IT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school IT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician and will be reviewed, at least annually, by the Online Safety Working Group.
- All users, for whom it is appropriate, will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames. Users will be required to change their password regularly.
- The "administrator" passwords for the school IT system, used by the ICT Technician must also be available to the Headteacher or School Business Manager and kept securely by the School Business Manager.
- The ICT Technician 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.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL.
- In the event of the ICT Technician needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Online Safety Coordinator and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Working Group.
- School ICT Technician regularly monitors and records the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy
- Any IT incident will be emailed to ICT Technician.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system. Any visitors who need access to the school system will be given temporary log in details by the ICT Technician. These details will be personalised and removed when no longer required.
- An agreed policy is in place regarding the downloading of executable files by users.
- An agreed policy is in place regarding the extent of personal use that users (staff/ pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that allows authorised staff to install programmes on school workstations/portable devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school workstations/portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring your own device (BYOD)

As a general rule, children can bring their own devices into school but not use them. Mobile phones or other devices should be locked away at the start of the day and returned before going home. However, a small number of children have use of their own tablets or iPads. These are used specifically to support communication and form part of a plan developed in conjunction with the class teacher, speech and language staff and parents / carers.

All equipment used in school is subject to the Online Safety Policy and relevant AUP, and has been passed to the ICT Technician prior to use in the classroom. Filtering settings and restrictions are applied to the device by the ICT Technician. All devices in school are subject to the same level of filtering, monitoring and restrictions as school devices.

Pupils' devices used in school are used only for specific purposes outlined in their speech and language programme. These devices are used under the supervision of classroom adults who are responsible for safeguarding other pupils against unauthorised photography or videoing.

Authorised programmes currently used at Mill Water consist of Proloquo2go and Grid Player.

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of IT across the curriculum.

- 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, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Technician 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.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line 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.

Use of digital and video images – photographic, video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment and the personal equipment of staff should not be used.

- Care should be taken when taking digital/video images that pupils 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 blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or shared with other parties.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

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

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

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed and identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- 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.

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 benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	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	✓							✓
Taking photos on mobile phones or other camera devices				✓				✓
Use of other mobile devices eg tablets, gaming devices		✓					✓	
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of chat rooms/facilities				✓				✓
Use of messaging apps				✓				✓
Use of social networking sites				✓				✓
Use of blogs	✓						✓	

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report to the Online Safety Coordinator the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and parents/carers (email, chat etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Staff and pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- 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 – Protecting Professional Identify

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; 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 on social media to pupils, parents/carers or school staff
- Their friends are not parents of pupils attending Mill Water School, or pupils
- No pictures of pupils attending Mill Water School are posted on social media sites
- 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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information or unwanted access

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Working Group to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate 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 school or outside school when using school equipment or systems. The school policy restricts certain internet 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					✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					✓	
Infringing copyright					✓	
Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, compute /network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational)		✓				
On-line gaming (non educational)					✓	
On-line gambling					✓	
On-line shopping/commerce			✓			
File sharing			✓			
Use of social media					✓	
Use of video broadcasting eg Youtube					✓	
Use of messaging apps					✓	

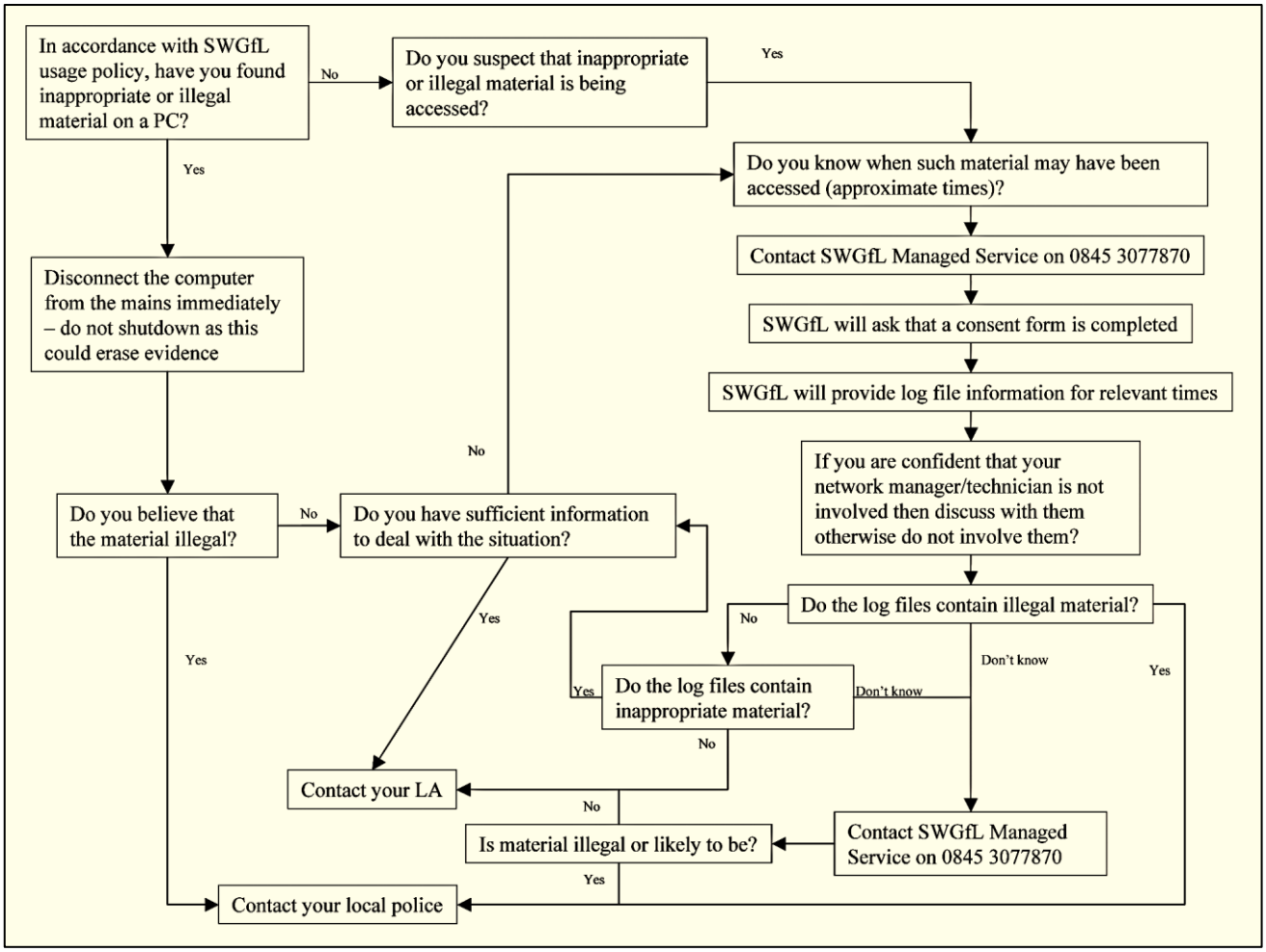
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of IT who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above), it is essential that correct procedures are used to investigate and preserve evidence, and protect those carrying out the investigation. In such event, the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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:

Pupils	**Actions / Sanctions**							
Incidents:	Refer to class teacher	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 sanction eg 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/digital camera/other handheld device	✓							
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 infringements 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 or 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 / Sanctions							
Incidents:	Refer to line manager	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).		✓	✓	✓				✓
Excessive or inappropriate personal use of the internet / social networking sites/instant messaging / 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 eg 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 instant message that is regarded as offensive, harassment or of a bullying nature		✓						✓
Using personal email/social networking/instant messaging / text messaging to carry out digital communications with pupils		✓						
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 or pornographic material and failing to report the incident		✓						✓
Deliberately accessing or trying to access offensive or pornographic material		✓						✓
Breaching copyright or licensing regulations		✓						
Continued infringements of the above, following previous warnings or sanctions		✓						✓

Mill Water School Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the South West Grid for Learning (SWGfL), schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Online Safety Coordinator. He will manage the school filtering, in line with this policy, and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the SWGfL / school filtering service that involve allowing a previously filtered site must:

- be logged and be reported to the Headteacher
- be reported to the Online Safety Governor annually

All users have a responsibility to report immediately to the Online Safety Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions, newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Online Safety Coordinator who will decide whether to make school level changes. If it is felt that the site should be filtered (or unfiltered) at SWGfL level, the Online Safety Coordinator should email filtering@swgfl.org.uk with the URL.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- Headteacher
- Online Safety Governor

The filtering policy will be reviewed in response to the evidence provided by the audit logs of the suitability of the current provision.

Mill Water School Password Security Policy

Introduction

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access.
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy.
- logs are maintained of access by users and of their actions while users of the system.

A safe and secure username / password system is essential if the above is to be established and will apply to all school IT systems, including email.

Responsibilities

The management of the password security policy will be the responsibility of the ICT Technician.

All users, other than those with group logons, will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users and replacement passwords for existing users can be allocated by the ICT Technician.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's Online Safety Policy and Password Security Policy
- through the Acceptable Use Agreement.

Pupils will be made aware of the school's password policy:

- in ICT and online safety lessons
- through the Acceptable Use Agreement.

Policy Statements

All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician and will be reviewed, at least annually, by the Online Safety Working Group.

All adult users will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames.

Some individual pupils will be allocated their own username and password. This will be determined by the Online Safety Coordinator. All other pupils will use a group log-on which will not be changed.

The following rules apply to the use of passwords:

- users accessing the s and t drive will change their passwords regularly
- pupils with their own log-ins will retain their passwords
- the password should be a minimum of 6 characters long and must include three of – uppercase character, lowercase character, number, special character
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords eg used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed
- requests for password changes should be authenticated by the ICT Technician to ensure that the new password can only be passed to the genuine user.
- The "administrator" password for the school IT system, used by the ICT Technician and SCOMIS staff must also be available to the Headteacher or other nominated senior leader and kept in the school safe.

Audit / Monitoring / Reporting / Review

The ICT Technician will ensure that full records are kept of:

- User IDs and requests for password changes
- User logons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by the Online Safety Working Group and Online Safety Governor annually.

This policy will be reviewed annually in response to changes in guidance and evidence gained from the logs.

Mill Water School Personal Data Handling Policy

Please refer to Mill Water School Data Protection Policy.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

14 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's laptops and iPads for schoolwork or with permission.
2. I will only delete my own files.
3. I will not look at other people's files without their permission.
4. I will keep my login and password secret.
5. I will not bring CDs, memory sticks or other devices into school without permission.
6. If I bring my mobile phone to school, I will keep it in a safe place and will not use it during the school day without permission.
7. I will ask permission from a member of staff before using the internet.
8. When I am at school I will only use the school email.
9. I will only e-mail people I know, or my teacher has approved.
10. The messages I send, or information I upload, will always be polite and sensible.
11. I will not open an attachment or download a file unless I have permission or I know and trust the person who has sent it.
12. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
13. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, carer or teacher has given me permission and I take a responsible adult with me.
14. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher/responsible adult.

Acceptable Use Policy for Pupils

Keeping Safe: Stop, Think, before you Click!

Pupil name:.....

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's laptops and iPads for schoolwork or with permission.
2. I will only delete my own files.
3. I will not look at other people's files without their permission.
4. I will keep my login and password secret.
5. I will not bring CDs, memory sticks or other devices into school without permission.
6. If I bring my mobile phone to school, I will keep it in a safe place and will not use it during the school day without permission.
7. I will ask permission from a member of staff before using the internet.
8. When I am at school I will only use the school email.
9. I will only e-mail people I know, or my teacher has approved.
10. The messages I send, or information I upload, will always be polite and sensible.
11. I will not open an attachment or download a file unless I have permission or I know and trust the person who has sent it.
12. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
13. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, carer or teacher has given me permission and I take a responsible adult with me.
14. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher/responsible adult.

- ✓ I have read the school '14 rules for responsible IT use'. My teacher has explained them to me.
- ✓ I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.
- ✓ This means I will use the school computers, laptops, internet, e-mail, digital cameras, video recorders and any other equipment in a safe and responsible way.
- ✓ I understand that the school can check my folders on the school network and the internet sites I visit and that if they have concerns about my safety, they may contact my parent/carer.
- ✓ I understand that if staff still have concerns about my safety, I might not be able to use the computers / laptops anymore.

Pupil's signature:..... Date:.....

Acceptable Use Policy for Parents / Carers

This Acceptable Use Policy is intended to ensure:

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

The school will try to ensure that pupils will have good access to IT to enhance their learning and will, in return, expect pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents 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

Parents / Carers name:.....

Pupil name:.....

As the parent/carer of the above pupil, I give permission for my son/daughter to have access to the internet and to IT systems at school.

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

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

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

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

Signature:..... Date:.....

Acceptable Use Policy for Staff and Volunteers

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 IT 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 IT in their everyday work.

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

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

For my professional and personal safety:

- I understand that the school will monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (eg laptops, email) out of school.
- I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I 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 IT 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. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school time.
- I will only communicate with parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (PDAs/laptops/mobile phones /USB devices etc) in school time, I will follow the rules set out in this agreement. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any hyperlinks or attachments to emails unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless authorised.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be password protected.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and, in the event of illegal activities, the involvement of the police.

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

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Acceptable Use Policy (normally an annual revisit).

I agree to abide by the school's most recent Acceptable Use Policy.

I wish to have an e-mail account, be connected to the internet and be able to use the school's IT resources and systems.

Signature:..... Date:.....

Full name:..... (printed)

Job title:.....

Authorised Signature

I approve this user to be set-up.

Signature:..... Date:.....

Full name:..... (printed)

Use of Digital Images – Photography and Video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/son.

We adhere to the following rules for any external use of digital images: If the pupil is named, we avoid using their photograph. If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils' work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that the pupils aren't referred to by name on the video and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity:

  e.g. photographing children at work and then sharing the pictures on the Interactive Whiteboard in the classroom allowing the children to see their work and make improvements.

- Your child's image being used for presentation purposes around the school:

  e.g. in school wall displays and PowerPoint presentations to capture images around the school or in the local area as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;

  e.g. within a CDROM/DVD or a document sharing good practice; in our school prospectus or on our school website.

- Your child's picture appearing in the local media such as newspaper articles about Mill Water, or in very rare cases on television if a film crew attends an event at the school.

- Your child's image being used by local organisations (who have worked with Mill Water) for their marketing purposes, such as the RNLI and the Fire and Rescue Service.

In accordance with guidance from the Information Commissioner's Office, parents and carers may take digital images and videos of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy, and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents and carers comment on any activities involving other pupils in the digital images or videos.

I have read and understood this document and I agree to the school using photographs of my child, including video material, within the school as part of learning activities and for presentation purposes around the school.

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

I also agree for images of my child to be used in the following ways (please tick to indicate your agreement):

YES ◯ NO ◯	In presentations about the school and its work in order to share good practice and celebrate its achievements, which may be shown to external audiences such as parents, schools and other educators.
YES ◯ NO ◯	On the school's website.
YES ◯ NO ◯	In local media such as newspaper articles about Mill Water, or in very rare cases on television if a film crew attends an event at the school.
YES ◯ NO ◯	By local organisations (who have worked with Mill Water) for their marketing purposes, such as the RNLI and the Fire and Rescue Service

Pupil name (s): .....

Parents / Carers signature: .....

Date: .....