Online Safety Policy

Guidance for staff regarding online safety
Good practice & guidelines

Policy Updated: September 2016

Policy Approved: .....

Policy Review Date: September 2017

Taken from SWGfL Education that Clicks

Background / 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
- Cyber-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 / Review of this Policy

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

- School Online Safety Coordinator – Lousia Rigsby
- Headteacher – Adam Richards
- Teachers - Clare Souch, Lauren Berry and Jo Smith
- Support Staff
- ICT Network Manager – Glyn Pascoe (iCT4 Ltd)

- Governors

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School council / pupils
- INSET Day
- Governors meeting
- Parents evening/discussions
- School website / newsletters

Schedule for Development / Monitoring / Review

This online safety policy was approved by the Governing Body:	Sept 2016
The implementation of this online safety policy will be monitored by the:	Online Safety Coordinator, Senior Leadership Team, Network manager & ICT technician
Monitoring will take place at regular intervals:	at least once a year
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	at least once a year
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:	Sept 2017
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Cornwall Council Child Protection Team / SWGFL, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
  - parents / carers
  - staff

Scope of the Policy

This policy applies to all members of Penponds school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Penponds School ICT 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 students / 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 out of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the 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 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 Governors receiving regular information about online safety incidents and monitoring reports. The role of the Online Safety Governor will include:

- 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 committee / meeting

Headteacher and Senior Leaders:

- **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-ordinator – Louisa Rigsby or Senior Leaders as necessary.
- **The Headteacher and another member of the Senior Leadership Team 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.** (see SWGfL flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures).
- Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders 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 network manager (iCT4 Ltd) will oversee the monitoring role within their SLA role.
- The Extended Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Coordinator:

- leads the Online Safety committee
- 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
- ensures that 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 Network Manager and technical staff (iCT4Ltd)
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with Online Safety Governor/headteacher to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Extended Leadership Team

Network Manager / Technical staff:

The Network Manager / IT Technician / ICT Co-ordinator is responsible for ensuring:

- that the school's ICT 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.
- *the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person* (see appendix "Filtering Policy Template" for good practice document)
- that 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
- that the use of the network / internet / Virtual Learning Environment (CLASS DOJO) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator (ICT Co-ordinator) / Headteacher / Senior Leader / Class teacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

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 Code of Conduct for Computing
- they report any suspected misuse or problem to the Online Safety Co-ordinator (ICT Co-ordinator) /Headteacher / Senior Leader / Class teacher 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
- online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school Online Safety Policy and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices in lessons, extra-curricular and extended school activities
- in lessons where internet use is pre-planned 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 (how to use google safe search on www, use of Hector and completion of online safety incident log).

Designated Safeguarding Lead (Headteacher)

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
- cyber-bullying

Online Safety Group

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinator with:

- the production / review / monitoring of the school Online Safety Policy.
- the production / review / monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision

- monitoring improvement actions identified through use of the 360-degree safe self-review tool

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement, which they will be expected to sign before being given access to school systems.
- eCadets (pupils from y3-6) will promote good eSafety practice across the school and community.
- 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 school policies on the use of mobile devices and digital cameras. They should also know and understand school 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 safe way. Research shows that many parents and carers do not fully understand the issues(digitally naïve) and are less experienced in the use of ICT than their children. The school and eCadets will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Twitter / Facebook / CLASS DOJO and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow the guidelines on the appropriate use of:

- **endorsing (by signature) the Pupil Acceptable Use Agreement (AUA)**
- digital and video images taken at school events
- accessing the school website / school Facebook page / school Twitter account / CLASS DOJO / on-line pupil records in accordance with the relevant school Acceptable Use Agreement.

Community Users

Community Users who access school systems / website / CLASS DOJO as part of the wider School provision will be expected to sign a Community User Acceptable Use Agreement before 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 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 should be a focus in all areas of the curriculum and staff with our eCadets 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 programme should be provided as part of Computing / PSHE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and 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 taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- 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.
- Rules for use of digital technologies / internet will be posted in all rooms
- Pupils should be helped to understand the need for the pupil AUA and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- 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 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 Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

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 may underestimate 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. "There is a generational digital divide". (Byron Report).

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

- Letters home 'Thinkuknow', newsletters, magazine (Digital Parenting), website – online safety page, CLASS DOJO
- Parents evenings and online safety briefings
- High profile events eg Safer Internet Day
- SWGFL "Golden Rules" for parents

Education – The Wider Community

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

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website, school Facebook and school Twitter account will provide online safety information for the wider community.

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 & Training – Staff / Volunteers

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. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.**
- **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 Coordinator will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by SWGfL / LA and others.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator / Network Manager 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 sub committee / group involved in technology / 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 (assemblies) 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 technical 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 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.** Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Committee.
- **All pupils will be provided with a username and password** by the Network Manager who will keep an up to date record of users and their usernames. KS1 will use class log-ons and passwords and be aware of the risks associated with shared access.
- **The "administrator" passwords for the school technical system, used by the Network Manager must also be available to the Headteacher or nominated senior leader and kept in a secure place.**
- 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 master/ administrator passwords for the school IT system used by the Network Manager must also be available to the Headteacher and kept in a secure place (eg. school safe)
- The school maintains and supports the managed filtering service provided by iCT4Ltd.

- **Internet access is filtered for all users.** Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- In the event of the Network Manager (or other person) 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 / online safety coordinator.
- Any filtering issues should be reported immediately to the online safety committee or Network Manager who will report to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager 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 Committee.
- School computing technical staff and ICT coordinator regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy. Penponds School uses iCT4 Ltd for filtering and monitoring services to monitor activity.
- The Network Manager 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.
- An appropriate system is in place (Online safety Incident Log Book) for users to report any actual / potential online safety incident to the Online Safety Coordinator and brought to the attention of the Headteacher, if necessary. Completed logs are to be kept in a locked place at all times.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.
- An agreed Acceptable Use Agreement for Guests is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) and Community Users (parents/carers /community users) onto the school systems. Staff are not to allow "**guests"** to use their login details.
- An agreed policy is in place regarding the downloading of executable files by users that the Network Manager is consulted before any installations are carried out to ensure that licences are upheld and security not breached.
- An agreed policy is in place regarding the extent of personal use that staff and their family members are allowed on laptops and other portable devices that may be used out of school. (see School Personal Data Policy)
- Installing programmes on school workstations / portable devices is not allowed unless agreed by the ICT coordinator, who will contact the Network Manager.
- An agreed policy is in place regarding the use of removable media (eg encrypted/password protected memory sticks / CDs / DVDs) by users on school workstations / portable devices. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.** (see School Personal Data Policy)
- The school infrastructure and individual workstations are protected by up to date virus software.
- Staff and Chair of Governors are to use their own school issued email address for all work related communication.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop 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's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- **The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies**

The school allows:

	School Devices		Personal Devices		
	School owned for single user	**School owned for multiple users**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*[1]	*Yes*[1]	*Yes*[3]
Full network access	*Yes*	*Yes*			
Internet only					
No network access					

[1] Authorised device – purchased by the family. Permission given by the teacher for the device to be used in the class. Teacher to evaluate the educational content and value before it is shared with other pupils i.e. sharing Bloom's Project Homework challenges. Storage of student owned device will be in the teacher's desk so it will be only used at the appropriate time. The student owned device may not be given full access to the network as if it were owned by the school.

[2] **Staff owned mobile devices will be allowed access to networks/internet if they are used for educational purposes and the meet the requirements of this policy:**

- **Filtering of the internet connection to these devices**
- **Data Protection**
- **Taking / storage / use of images**
- **The right to take, examine and search users devices in the case of misuse (England only) – n.b. this must also be included in the Behaviour Policy.**

[3]**The use of Guest mobile devices in school: may be allowed access to networks/internet if they are used for educational/training purposes and the meet the requirements of this policy:**

- **Complete a Guest Acceptable User Agreement**
- **Filtering of the internet connection to these devices**
- **Data Protection**
- **No taking / storage / use of images**
- **The right to take, examine and search users' devices in the case of misuse (England only) – n.b. this must also be included in the Behaviour Policy.**

Curriculum

Online safety should be a focus in all areas of the curriculum and staff and eCadets should reinforce online safety messages in the use of digital technology 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 safe search engines, staff should be vigilant in monitoring the content of the websites the pupils 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 Network Manager (and other relevant 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.
- 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, parents / carers and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Such images may provide avenues for cyberbullying to take place. 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 such as Facebook and Twitter.**
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment (not mobile phone cameras) of staff may **only** be used with permission of the Headteacher under certain circumstances and the images are to be downloaded onto the school network and then deleted off the personal equipment.
- 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 *pupils* in the digital / video images.
- 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 school website, newsletters, school and class Twitter accounts, class blog or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Photographs and names of pupils will not be used on the school Facebook page.
- Pupils' full names will not be used anywhere online- school website, school Twitter accounts or class blog, no pupil names will be used in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/school social media/local press-see Parents / Carers Acceptable Use Agreement.
- 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 / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **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 or "locked" when idle within a session. Staff computers to be 'locked' when leaving the room, only to be unlocked with password.**
- **Transfer data using encryption and secure password school issued protected devices.**

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

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

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 – for explicit educational purposes		✓				✓		
Use of mobile phones in social time		✓						✓
Taking photos on school owned camera devices- NOT MOBILE PHONES	✓				✓			
Use of school owned mobile devices eg iPads	✓				✓			
Use of personal email addresses in school, or on school network only ***after school clubs have finished***	✓							✓
Use of school email for personal emails - Use your professional judgement		✓						✓
Use of chat rooms /facilities-for educational purposes ONLY (CLASS DOJO)		✓					✓	
Use of messaging APPS				✓				✓
Personal use of social media (such as Facebook)				✓				✓
Use of Penponds School Facebook page for information/communication purposes			✓					✓
Use of Penponds School Twitter Account for educational/information purposes			✓					✓
Use of Class Twitter Account for educational and information purposes **TEACHER TO APPROVE TWEETS BEFORE THEY ARE TWEETED.**		✓					✓	
Use of blogs-for educational purposes ONLY	✓					✓		

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 – in accordance with the school policy, 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 pupils or parents / carers (email, chat, CLASS DOJO, Twitter etc) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- 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, school /class Twitter accounts or school Facebook page and only official email addresses should be used to identify members of staff.

Social Media – Protecting Professional Identity

All schools, academies 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.

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 access to personal information:

- Ensuring that personal information is not published.
- 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 in personal 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 – Head teacher and will regularly check school and class twitter account*
- *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, including*
- *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 the school 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

Montitoring 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

The *school's* use of social media for professional purposes will be checked regularly by the Headteacher and *Online Safety Coordinator* to ensure compliance with the school policies and inappropriate comments.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school /academy 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 school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

ser 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**					✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation -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/pupils 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 the school					✓	
Infringing copyright-uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Unfair usage-carrying out sustained or instantaneous high volume network traffic (downloading/uploading large files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational)			✓			
On-line gaming (non educational) for Golden Time or Super Sixes privileges only			✓			

On-line gambling				✓	
On-line shopping /commerce for Teachers - outside teaching hours ONLY for personal use		✓			
File sharing - internal use for educational use		✓			
Use of social networking sites (such as Facebook) for personal use				✓	
Use of video broadcasting for educational purposes eg Teachertube NOTE: Youtube is unfiltered; Media needs to be fully audited before sharing with pupils.		✓			

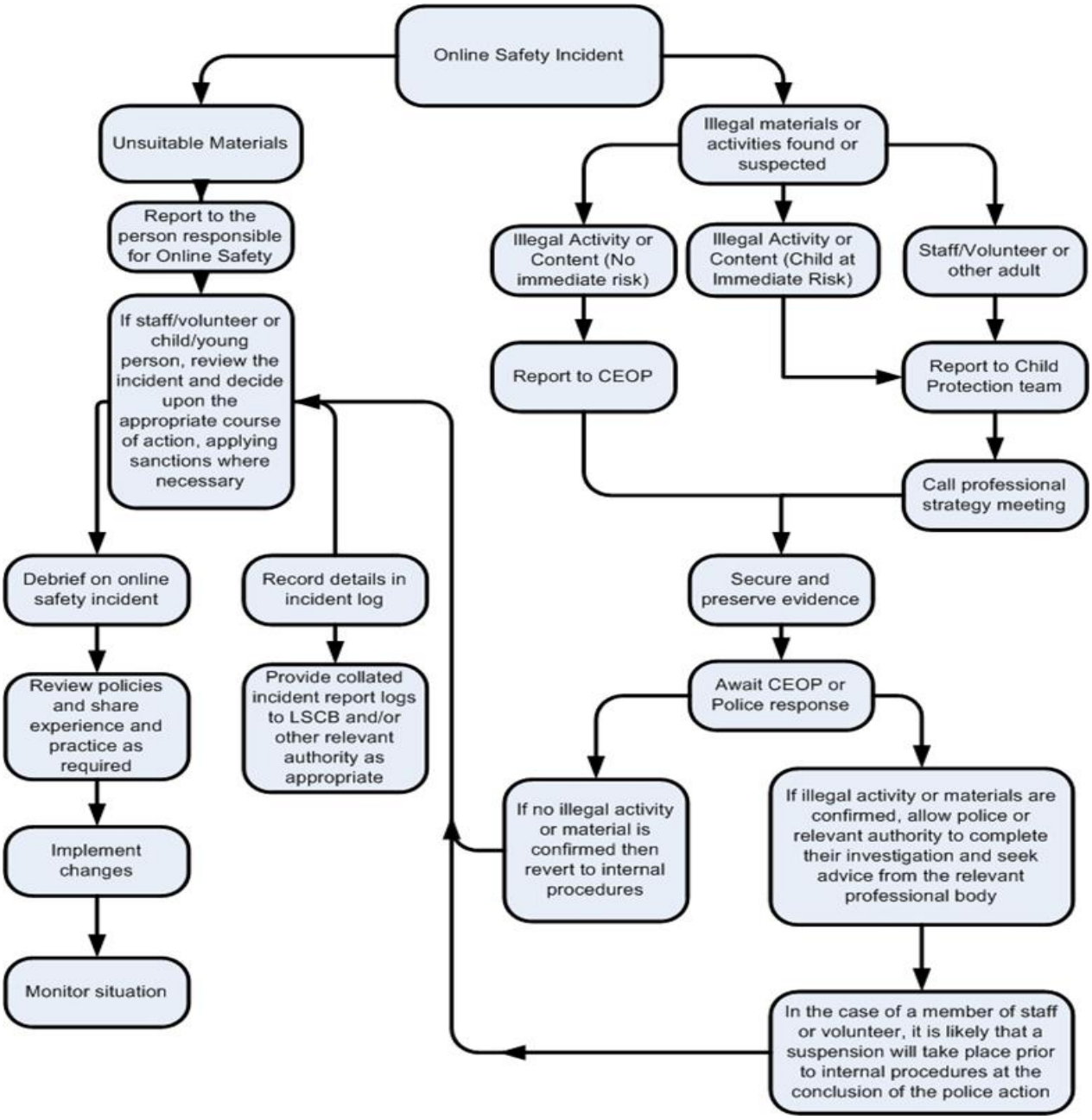
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of digital technology, 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**
- **Promotion of extremism or terrorism**
- **other criminal conduct, activity or materials**

The flow chart – below 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.



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 or 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 / volunteer 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 young people 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
    - Promotion of extremism or terrorism
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

School Actions and Sanctions

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:

Actions / Sanctions

Pupils Incidents:	Refer to class teacher	Refer to Headteacher	Headteacher to consider further actions:	-Refer to Police	-Refer to technical support staff for action re filtering /	-Inform parents / carers	-Removal of network / internet access rights	-Warning	-Further sanction eg 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 / digital camera / other handheld device	✓	✓				✓					
Unauthorised use of social networking / instant messaging / 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 student's / 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 instant 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 Incidents:	Refer to Online safety Coordinator	Refer to Headteacher	Refer to Governors	Headteacher to consider further actions	-Refer to Local Authority / HR	-Refer to Technical Support Staff for action re filtering etc	-Refer to Police	-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 during school hours	✓	✓	✓	✓						
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 carrying out digital communications with students / 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. For example: Mentioning work related incidents on social networking sites.		✓	✓	✓						
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		✓	✓	✓						

Appendices

- Online safety - A Charter for Action
- Pupil Acceptable Use Agreement and Parental / Carer Permission
- Parent/Carer permission for photographs on website and press
- Staff and Volunteer Acceptable Use Policy Agreement
- Staff iPad Acceptable Use Policy
- iPad Rules for class room display
- Community User Acceptable Use Agreement
- Guest Acceptable Use Agreement
- SWGFL online safety processes
- Online safety Incident Log
- Record of reviewing devices/internet sites (responding to incidents of misuse)
- Training Needs Audit
- Social Media Policy
- Twitter Policy
- Resources
- Legislation
- Cyberbullying Policy
- School Personal Data Handling Policy
- Privacy Notice – pupils in schools

Online Safety
A School Charter for Action

Penponds Primary School

Rainbow Multi Academy Trust

We are working with staff, pupils and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of digital technologies, and follows agreed policies to minimise potential online safety risks.

Our school community

Discusses, monitors and reviews our Online Safety policy on a regular basis. Good practice suggests the policy should be reviewed annually.

Supports staff in the use of digital technology as an essential tool for enhancing learning and in the embedding of online safety across the whole school curriculum.

Ensures that pupils are aware, through online safety education, of the potential online safety risks associated with the use of digital and mobile technologies, that all online safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's online safety policy.

Provides opportunities for parents/carers to receive online safety education and information, to enable them to support their children in developing good online safety behaviour. The school will report back to parents / carers regarding online safety concerns. Parents/carers in turn work with the school to uphold the online safety policy.

Seeks to learn from online safety good practice elsewhere and utilises the support of SWGfL and relevant organisations when appropriate.

Chair of Governors	
Headteacher	
eCadets	

Computing Acceptable Use Agreement for Pupils and Parents

Penponds Primary School has installed computers, mobile devices and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

☺ I will access the system with my login and password, which I will keep secret.

☺ I will not access other people's files without permission.

☺ I will only use the digital devices for school work and homework unless I have permission for recreational use.

☺ I will not bring in software or personal devices into school without permission.

☺ I will ask permission from a member of staff before using the Internet.

☺ I will only e-mail people I know, or people that my teacher has approved.

☺ I will not open e-mails sent by someone I don't know.

☺ The messages I send will be polite and responsible.

☺ I will never give out personal information about myself or others such as; full names, home addresses or telephone numbers, or arrange to meet anyone.

☺ I will report any unpleasant material or messages sent to me.

☺ I understand that the school may check my computer files and may monitor the Internet sites I visit.

☺ I will not use Internet chat-rooms in school

☺ I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

I agree to follow the computing rules above.
Signed by child

_____

I understand that my son's / daughter's activity on the school system will be monitored and that the school will contact me if they have concerns about 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.

Signed by parent/guardian

_____ Date_____

Dear Parents / Carers,

We are updating our Data Protection records, and would appreciate all parents/carers to once again give their permission for photographs and video clips to be used for school purposes on our school website, school/class Twitter and/or school publications or in the local press.

We would like to thank you for your continued support,

Mr Adam Richards — Headteacher

Mrs Lousia Rigsby — Online safety Co-ordinator

Conditions of use

This form is valid for the period of time your child attends this school. The consent will automatically expire after this time.

We will not re-use any photographs or recordings after your child leaves this school.

We will not use the personal details or full names (first name and surname) of any child in a photographic image or video on our website, school/class Twitter Account, in our school prospectus or in any of our other printed publications.

If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption.

If we name a pupil in the text, we will not use a photograph of that child to accompany the article.

We may include pictures of pupils and teachers that have been drawn by the pupils.

We may use group or class photographs or footage with very general labels, such as 'a science lesson' or 'making Christmas decorations'.

I agree that Penponds School can use images and video clips of my child in it's school publications, school/class Twitter account and on the school website. I am happy for the press to take and use images of my child as part of Penponds school life with their first name only. YES / NO

Name of child ……

Class …….. Date ……

Signed……

Staff and Volunteer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times. To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this Acceptable Use Policy Agreement. Members of staff should consult the school's Online Safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school computing system for a purpose not permitted by its owner.
- I appreciate that computing includes a wide range of systems, including mobile phones, iPads, digital cameras, email, social networking and that Computing use may also include personal digital devices when used for school business.
- I will not bring the school into disrepute or breach the integrity of the ethos of the school. For example, mention work related incidents or post work related photographs on social networking sites.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely on school provided encrypted devices and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Online Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will ensure that electronic communications with pupils including email, tweets and CLASS DOJO are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote Online Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
I have read, understood and accept this Acceptable Use Policy Agreement.

Signed:…… Print name: ..... Date: .....

Penponds School iPad Acceptable Use Policy

User Responsibilities

- The iPad screen is made of glass and is therefore subject to cracking and breaking if misused; never drop or place heavy objects (book, laptops etc) on top of the iPad.
- Users must use protective cases/covers for their iPad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extremes of temperature.
- Do not store or leave unattended in vehicles.

Safeguarding and Maintaining as an Academic Tool

- Users may not photograph any other person without that person's consent
- Photographs of children must be in line with Consent Letter Agreement
- The whereabouts of the iPad should be known at all times.
- It is a user's responsibility to keep their iPad as safe and secure as possible.

Prohibited Uses

- Images of other people may only be made with the permission of the person, or parents of the person, in the photograph.
- The iPad should always be available in school to enhance classroom practice. It is not for personal use of social networking sites.

Lost, Damaged or Stolen iPad

- If the iPad is lost, stolen or damaged, the ICT Subject Leader or Head Teacher must be informed immediately.

Please read and sign below:
I have read, understand and agree to abide by the terms of the iPad Acceptable Use Policy.

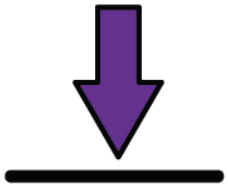
Name:

Signature:

Date:

OUR IPAD RULES

Hold the iPad with two hands.

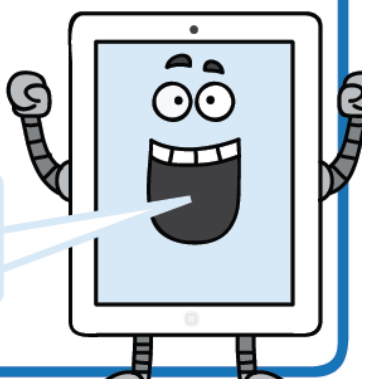


Always sit down when using the iPad.

Turn the iPad's screen off when the teacher is talking.

Be gentle when tapping the screen.

Only use the app or website you have been asked to use.



Be Safe ... Be Responsible ... Be Respectful...

Community Users Acceptable Use Agreement

For use by any Community User using our computing devices in the school for a short period of time.

Penponds Primary School has installed computers, iPads and Internet access to help our pupils learning. These rules will keep everyone safe and help us be fair to others.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- I will not browse, download/upload or distribute any material that could be considered offensive, criminally racist material, pornographic, illegal or discriminatory. 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 respect copyright and intellectual property rights.
- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I will not install any hardware or software onto any school system.
- 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 understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.
- 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 have read and agree to follow this code of conduct and to support the safe use of information communication technology throughout the school.

User Signature _____ Date _____

Full Name _____ (PRINT)

Position/Role _____

Guest Acceptable Use Agreement

For use by any adult working in the school for a short period of time.

Penponds Primary School has installed computers, iPads and Internet access to help our pupils learning. These rules will keep everyone safe and help us be fair to others.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- I will not browse, download/upload or distribute any material that could be considered offensive, pornographic, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I will ensure that images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I will not install any hardware or software onto any school system.
- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

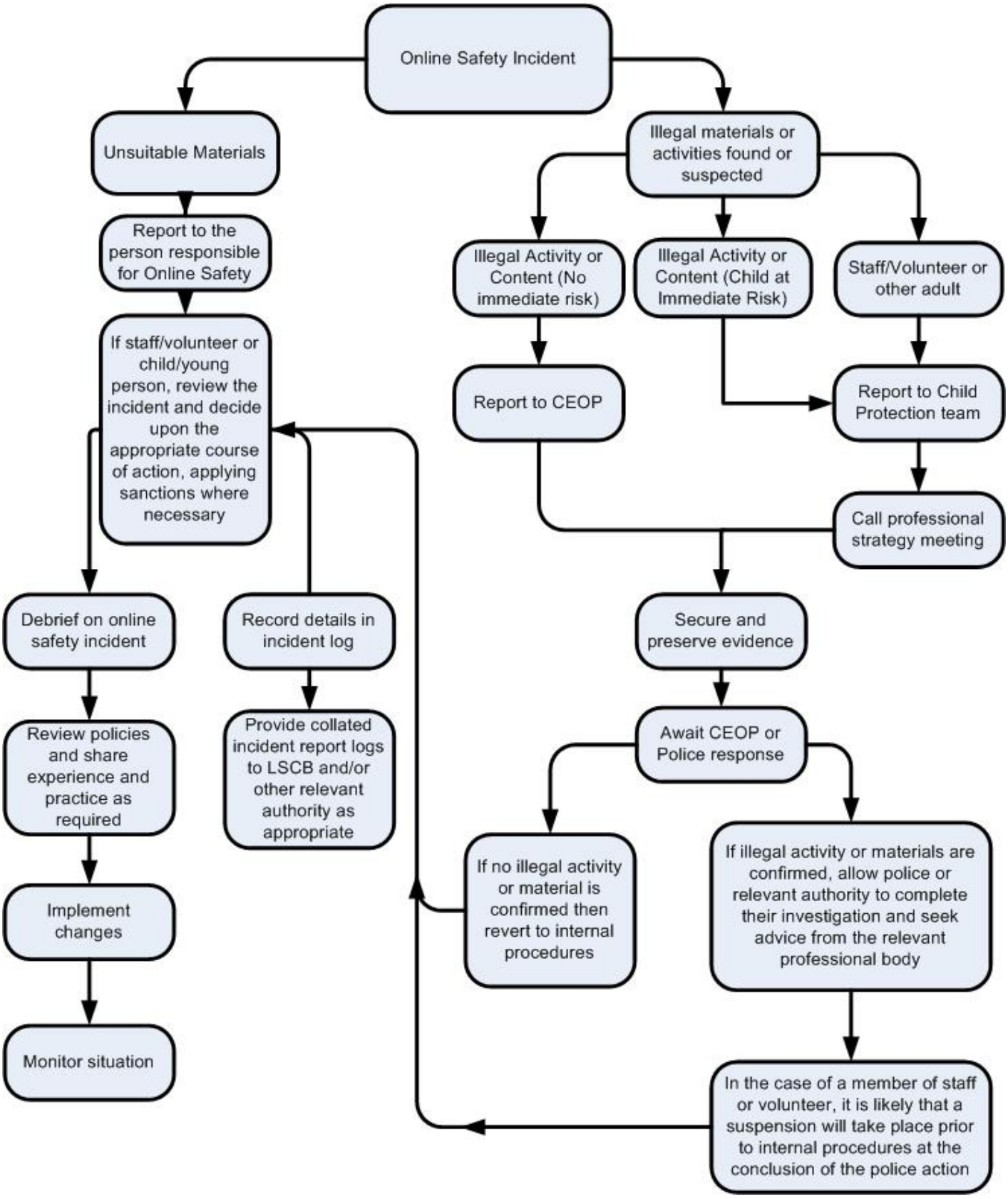
I have read and agree to follow this code of conduct and to support the safe use of computing technologies throughout the school.

User Signature _____ Date _____

Full Name _____ (PRINT)

Position/Role _____

Responding to incidents of misuse – flow chart



Online Safety Incident Log

All online safety incidents must be recorded by the Online Safety Coordinator or Headteacher This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors. Any incidents involving CYBERBULLYING should also be recorded on the Integrated Bullying and Harassment Incident Form.

Date /Time of Incident	Type of Incident	Name of pupil/s and staff involved	System Details	Incident details	Resulting actions taken and by whom (and signed)
01 Jan 2010 9.50am	Accessing Inappropriate Website	A.N Other – pupil AN Staff class teacher	Class1 Computer 1.5	Pupil observed by Class Teacher deliberately attempting to access adult websites	Pupil referred to Headteacher and given warning in line with 1st time infringement of AUP. Site reported to SWGFL as inappropriate

Only ONE incident per Online Safety Incident Log page. Please hand immediately to Online Safety Coordinator or Headteacher. This completed log is to be kept in a locked place.

Record of reviewing devices/internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer/mobile device used for review (for websites)

Website(s) address/device Reason for concern

Conclusion and Action proposed or taken

Training Needs Audit Log

Group .....

Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date

Social Media Policy

Policy Updated: **September 2016**

Policy Approved: **.....**

Policy Review Date: **September 2017**

Social media (e.g. Facebook, Twitter, Instagram, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as YouTube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school 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.

Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- **SLT**
    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Receive completed applications for Social Media accounts
    - Approve account creation

- **Administrator / Moderator**
    - Create the account following SLT approval
    - Store account details, including passwords securely
    - Be involved in monitoring and contributing to the account
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
    - Attending appropriate training
    - Regularly monitoring, updating and managing content he/she has posted via school accounts
    - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts
The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy.** Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.

- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy.** If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school 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.*
- **Pupil/Students**
    - **Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.**
    - The school's education programme should enable the pupils/students to be safe and responsible users of social media.
    - Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
    - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
    - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
    - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- 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.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private

- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Twitter Policy

Policy Updated: Sept 2016

Policy Approved: .....

Policy Review Date: Sept 2017

What is Twitter?

Twitter is a form of social media which allows users to send and read 140-character messages or 'Tweets'. These might be simple messages or announcements or may include pictures or links to other sites on the internet. Users access Twitter either through the website (there is a link and feed to this on www.Penponds.cornwall.sch.uk) or by using the app on a mobile device (e.g. an iPad/iPhone or Android equivalent). Tweets can be viewed via the internet without signing up or users can create a Twitter account to 'follow' certain people or organisations. Penponds CP School recognises that access to class/school Twitter accounts gives pupils and staff greater opportunities to learn, engage, communicate and develop skills that will prepare them for work, life and citizenship.

Why use Twitter in school?

Many UK schools are using Twitter, we have successfully trialled an account: @PenpondsSchool. The uses of Twitter are endless but some examples include:

- Celebrating achievement – of individuals, teams and the whole school.
- Collaborating with pupils and teachers in other schools.
- Updating the school community about school events and news (including links to our school website).
- Engaging our pupils by connecting with people all over the world including authors, industry experts, scientists, sports people and astronauts.
- Engaging the whole school community in discussion about what matters in our school.
- Giving our pupils an insight into, and stimulating conversation about events and issues around the world that matter to them.

Penponds CP School Twitter handles

@Penponds_School	whole school account
@Carn_Brea_Penponds	reception/year 1 class
@Godophin_Penponds	Y1/2
@Trencom_Penponds	Y3/4
@Tregonning_Penponds	Y5/6

Is it safe?

We strongly believe that part of our role in the technological age we are learning in is to educate our pupils to use forms of social media such as Twitter effectively and safely. Tweets will only be posted by adults in school and anyone who the school or class choose to follow will be closely scrutinised beforehand to assess their suitability.

Aims of Using Twitter:

- To share and celebrate children's achievements and successes
- To allow our pupils to connect with the world
- To demonstrate safe and responsible use of social media
- To update the school community on a range of issues
- To encourage the use of 21st Century technology

- The school and class Twitter accounts will be public accounts. The online safety coordinator will monitor school and class followers and block those who appear to not be school focused.

- Class Twitter will only ever be controlled by teachers working at Penponds CP School. Pupils will have the chance to write Tweets and help select who their class 'follows' but both of these will always be vetted by teaching staff beforehand. Twitter users must be 13+ years of age.

- Class Twitter accounts will only follow other accounts that teaching staff agree are both suitable (based both on knowledge of the account holder and from previous 'Tweets') and of educational merit.

- School / Class Twitter accounts will never include named photos and names of pupils in the same Tweet (it will be either / or). Parents have the right to request for their child not to appear in any Tweets either by name of photo, such requests should be made in writing through the school office or their child's Class Teacher.

- The Penponds CP School community uses Twitter with a firm knowledge of the potential dangers associated with social networking. This means that Class Teachers take every opportunity to discuss safety issues related to the use of Twitter and model these in their use of all forms of ICT.

- Class/school Twitter accounts will be in the Public domain. So while tweets and comments from parents and followers are actively encouraged; inappropriate language or photographs may result in an account being blocked by the school.

- We make all efforts to ensure pupils' safety and security online, but will not be held accountable for any harm or damages that result from misuse of a class/school Twitter account.

- Staff should avoid using their own equipment to tweet in school unless learning off-site and need to use an alternative internet connection to send a class/school tweet - for school purposes only.

- Twitter's own safety rules can be read on: https://support.twitter.com/groups/57-safety-security#topic_271

What is inappropriate content and referencing and how it will be dealt with?

Our school welcomes any referencing, mentions or interactions that promote the school in a positive light only. Therefore, Penponds CP School deems any of the following as inappropriate:

- Offensive language or comments aimed at the school, its staff, parents, governors or others affiliated with the school.
- Unsuitable images or content posted into its feed.
- Unsuitable images or content finding its way from another's account into our school Twitter accounts.
- Images or text that infringes upon copyright.
- Comments that undermine the school, its staff, parents, governors or others affiliated with the school.

Any inappropriate content will be deleted and its users will be removed, blocked and depending on the comment reported to Twitter. Incidents of a more serious nature may be reported to the appropriate authority.

Guide to Twitter

Tweet:	A 140-character message.
Retweet (RT):	'Quoting' or reposting someone else's tweet you think might be of interest to others. RT usually precedes the original post to give credit to the user who published it first. (Source: @UKEdChat)
Feed	The stream of tweets you see on your homepage. It's comprised of updates from users you follow.
Handle	Your username (e.g. '@PenpondsSchool')
Mention/Reply(@)	A way to reference another user by their username in a tweet. Users are notified when @mentioned. It's a way to conduct discussions with other users. If you are replying to a tweet and want everyone to see your response, place a full-stop/period prior to the user name .@ukedchat
Hashtag (#)	A way to denote a topic of conversation or participate in a larger linked discussion (e.g. #edchat). You can also click on a hashtag to see all the tweets that mention it in real time — even from people you don't follow.
DM	This is a private Direct Message sent to a twitter user. You must follow that user before you can message them. DMs don't appear in the public twitter stream.
Follow	These are the accounts you are following and the tweets will appear in your time-line.
Follower	Someone who follows you and your tweets. Be grateful for any feedback.
Link	Including a URL in your tweet. You can use shortened URL services, such as bit.ly although twitter mainly shortens URLs automatically now.

Getting started . . .

1. Create an account – decide on your 'handle' (e.g. @PenpondsSchool), upload a photo and add a short 'bio' so people have an idea of who you are (e.g. 'We are Tregonning Class, a year 5/6 class at Penponds School).

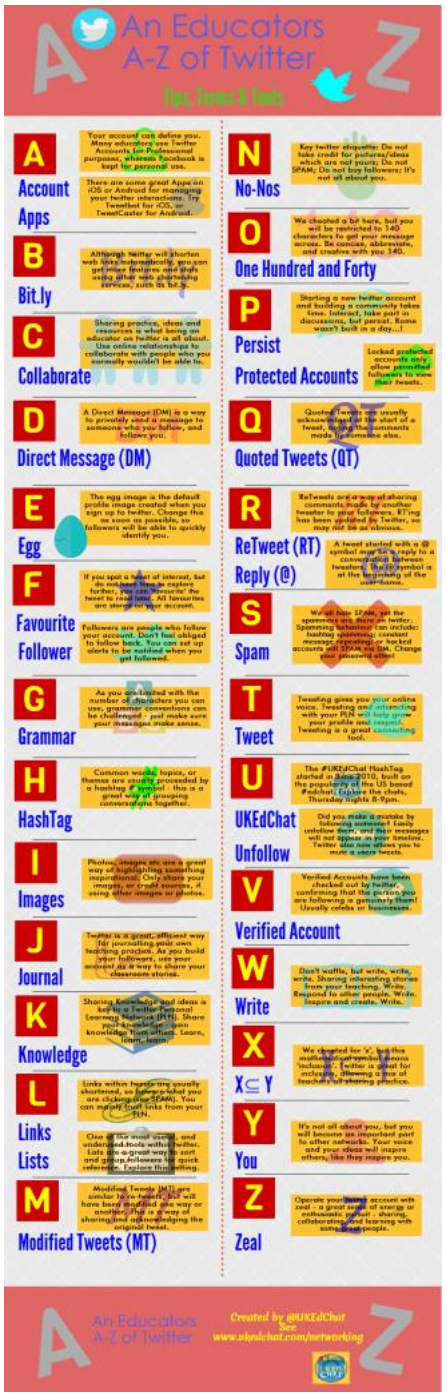
2. Decide who to follow – you can find other Twitter uses to begin with by using the search function. Once you've found who you're looking for, simply click 'follow' and all their Tweets will automatically appear on your 'feed' (your feed is part of the Twitter app or website so you will not be notified of other people's Tweets (like you might a text message for example) unless you request this for any user you are following).

Who you follow is clearly down to what you want to get out of the Twitter experience. Many classes choose to follow various authors or poets; others find it a really use tool for keeping informed on various issues by following other classes, schools and organisations such as NASA. Once you are following a number of other users, Twitter will become more intuitive in suggesting others that might be of interest.

3. Tweet! – Start small with simple messages, gradually including hashtags such as #maths in each of your tweets. As you are limited with the number of characters you can use, grammar conventions can be challenged - just make sure your messages make sense. Find a class from another school and share # to interact with each other.

A popular way to enter the Twitter for the first time is to 'Retweet' a comment from someone else. This is a bit like quoting someone else and will be done primarily because you want people who follow you to see it. It will appear on your personal feed but with the original author credited with the Tweet.
For lots more information visit https://support.twitter.com/groups/50-welcome-to-twitter

Twitter infographic - http://ukedchat.com/2014/06/16/resource-an-a-z-of-twitter-for-educators/



Cyberbullying Policy

Policy Updated: Sept 2016

Policy Approved: .....

Policy Review Date: Sept 2017

Taken from Cornwall Council

CYBERBULLYING

What is cyberbullying?

"Cyberbullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself."[2]
Seven categories of cyberbullying have been identified:

- Text message bullying involves sending unwelcome texts that are threatening or cause discomfort.
- Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks.
- Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
- Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- Chat room bullying involves sending menacing or upsetting responses to children or young people when they are in a web-based chat room.
- Bullying through instant messaging (IM) is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online.
- Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyberbullying.

What can schools do about it?

While other forms of bullying remain prevalent, cyberbullying is already a significant issue for many young people. Penponds School recognise that staff, parents and children need to work together to prevent this and to tackle it whenever it occurs.

School Governors, Head teachers and schools have a duty to ensure that:
bullying via mobile phone or the Internet is included in their mandatory anti-bullying policies, that these policies are regularly updated, and that teachers have sufficient knowledge to deal with cyberbullying in school[3].
Penponds School ensures that:

- the curriculum teaches pupils about the risks of new communications technologies, the consequences of their misuse, and how to use them safely including personal rights
- all e-communications used on the school site or as part of school activities off-site are monitored
- clear policies are set about the use of mobile phones at school and at other times when young people are under the school's authority
- Internet blocking technologies are continually updated and harmful sites blocked
- they work with pupils and parents to make sure new communications technologies are used safely, taking account of local and national guidance and good practice
- security systems are in place to prevent images and information about pupils and staff being accessed improperly from outside school

[2] Research commissioned by the Anti-Bullying Alliance from Goldsmiths College, University of London
[3] The School Standards and Framework Act 1998 require schools to have anti bullying policies; the anti bullying policy should include or refer to a cyberbullying policy. The ICT policy should also refer to cbyerbullying

- they work with police and other partners on managing cyberbullying.

ICT and Mobile Phone Policy

If a cyberbullying incident directed at a child occurs using e-mail or mobile phone technology, either inside or outside school time, Penponds School will take the following steps:

- Advise the child not to respond to the message
- Refer to relevant policies, e.g. online safety/acceptable use, anti-bullying and PSHE and apply appropriate sanctions
- Secure and preserve any evidence
- Inform the sender's e-mail service provider
- Notify parents of the children involved
- Consider delivering a parent workshop for the school community
- Consider informing the police depending on the severity or repetitious nature of the offence. The school recognises that some cyberbullying activities could be a criminal offence under a range of different laws including: the Protection from Harassment Act 1997; the Malicious Communication Act 1988; section 127 of the Communications Act 2003 and the Public Order Act 1986
- Inform the SWG4L lead: Jane McFall: 01872 322765

If malicious or threatening comments are posted on an Internet site or Social Networking Site about a pupil of member of staff, Penponds School **will also:**

- Inform and request that the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Send all the evidence to www.ceop.gov.uk/contact_us.html if of a sexual nature
- Endeavour to trace the origin and inform the police as appropriate.
- Inform the SWG4L lead: Jane McFall 01872 322765

Working with Parents

Penponds School will develop a home-school agreement that includes clear statements about e-communications. The school seeks to regularly update parents on:

- What to do if problems arise
- E-communication standards and practices in school
- What's being taught in the curriculum
- Supporting parents and pupils if cyberbullying occurs by:
  - ✓ Assessing the harm done
  - ✓ Identifying those involved
  - ✓ Taking steps to repair harm and to prevent recurrence

Code of Conduct

Penponds School have developed an ICT acceptable use policy with our pupils.

School Personal Data Handling Policy

Policy Updated: Sept 2016

Policy Approved: .....

Policy Review Date: Sept 2017

Taken from SWGFL

School Personal Data Handling Policy

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office –for the school and the individuals involved. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority. Guests and visitors to Penponds school who will be using the ICT system will have to sign the Guest ICT AUP.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

The DPA defines "Personal Data" as data which relate to a living individual who can be identified (http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions)

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines "Sensitive Personal Data" as personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- his political opinions
- his religious beliefs or other beliefs of a similar nature
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

Guidance for organisations processing personal data is available on the Information Commissioner's Office website: http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Fair Processing Code" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents and carers eg names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

Responsibilities

The school's Senior Risk Information Officer (SRIO) is Steve Medlyn. They will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (eg pupil / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand:

- what information is held and for what purpose
- how information as been amended or added to over time
- who has access to protected data and why

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the Privacy Notice

Under the "Fair Processing" requirements in the Data Protection Act, the school will inform parents / carers of all pupils / students of the data they hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DCSF, QCA, etc) to whom it may be passed. This fair processing notice will be passed to parents / carers through a letter which will also be located on the School Website. Parents / carers of children who are new to the school will be provided with the fair processing notice through a *letter, the contents are below:*

Privacy Notice - Data Protection Act 1998

We Penponds School are the Data Controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information[1] and personal characteristics such as your ethnic group, special educational needs and any relevant medical information. *If you are enrolling for post 14 qualifications we will be provided with your unique learner number by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.*

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some of your information to the Local Authority and the Department for Education (DfE). If you want to see a copy of the information we hold and share about you then please contact Mrs Lamb or please write to the school requesting the information. If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:
http://www.cornwall.gov.uk/default.aspx?page=20730
http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites, please contact the LA or DfE as follows:

- The Local Authority's Data Protection Officer can be contacted at **Cornwall Council, County Hall, Truro, Cornwall, TR1 3AY**
  Website: www.cornwall.gov.uk
  Telephone: 0300 1234 101

- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London SW1P 3BT
  Website: www.education.gov.uk
  email: http://www.education.gov.uk/help/contactus

  Telephone: 0870 000 2288

Attendance is not collected for pupils under 5 at Early Years Settings or Maintained Schools

Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners.

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Identification of data -Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data.

The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
Not Protectively Marked	0	Will apply in schools
Protect	1 or 2	
Restricted	3	
Confidential	4	Will not apply in schools
Highly Confidential	5	
Top Secret	6	

Impact levels are as follows:

- IL1–Not Protectively Marked (IL1–NPM)
- IL2–Protect (data that could cause embarrassment to pupils and their family, commercial interests and to School and its staff.) Only encrypted data can leave the School site.
- IL3–Restricted (SEN and Medical Records are not to leave the School site)
- IL4–Confidential

The following provides a useful guide:

	The information	**The technology**	**Notes on Protect Markings (Impact Level)**

School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer:

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g.. "Securely delete or shred this information when you have finished using it". .3

[Release]	[Parties]	[Restrictions]	[Encrypt, Securely delete or shred]
The authority descriptor	The individuals or organisations the information may be released to	Descriptor tailored to the specific individual	How the document should be destroyed
Examples:			
Senior Information Risk Owner	School use only	No internet access No photos	Securely delete or shred
Teacher	Mother only	No information to father-ASBO	Securely delete or shred

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

All users will be given secure user names and strong passwords (capital and lowercase letters, numbers and punctuation) which must be changed regularly every 30 days. User names and passwords must never be shared.

Personal data may only be accessed on machines (staff computers) that are securely password protected. Any device that can be used to access data must be properly "logged-off" at the end of any session or "locked" when idle within a session - only to be unlocked with password.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media) (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.

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

- **the data must be encrypted and password protected**
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups that are managed by the Network Manager.

All paper based IL2-Protected and IL3-Restricted (or higher) material must be held in lockable storage.

The school recognises that under Section 7 of the Data Protection Act, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests ie. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

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 restricted or protected personal 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. (For example: - to carry encrypted material is illegal in some countries)

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained at evidential quality for seven years.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Further reading

Teachernet – Data processing and sharing -
http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/

Office of the Information Commissioner website:
http://www.informationcommissioner.gov.uk

Office of the Information Commissioner – guidance notes: Access to pupil's information held by schools in England

Becta – Good Practice in information handling in schools – keeping data secure, safe and legal and it's four detailed appendices: (September 2008)

http://schools.becta.org.uk/upload-dir/downloads/information_handling.pdf

http://schools.becta.org.uk/upload-dir/downloads/information_handling_impact_levels.pdf

http://schools.becta.org.uk/upload-dir/downloads/data_encryption.pdf

http://schools.becta.org.uk/upload-dir/downloads/audit_logging.pdf

http://schools.becta.org.uk/upload-dir/downloads/remote_access.pdf

Cabinet Office – Data handling procedures in Government – a final report (June 2008)
http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

PRIVACY NOTICE

Pupils in Schools

Privacy Notice - Data Protection Act 1998

We, Penponds School are the Data Controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information[1] and personal characteristics such as your ethnic group, special educational needs and any relevant medical information. *If you are enrolling for post 14 qualifications we will be provided with your unique learner number by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.*

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some of your information to the Local Authority and the Department for Education (DfE). If you want to see a copy of the information we hold and share about you then please contact Mrs Lamb or please write to the school requesting the information. If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

http://www.cornwall.gov.uk/default.aspx?page=20730
http://www.education.gov.uk/schools/adminandfinance/schooladmin/ims/datamanagement/privacynotices
http://media.education.gov.uk/assets/files/doc/w/what%20the%20department%20does%20with%20data%20on%20pupils%20and%20children.doc

If you are unable to access these websites, please contact the LA or DfE as follows:

- The Local Authority's Data Protection Officer can be contacted at **Cornwall Council, County Hall, Truro, Cornwall, TR1 3AY**
  Website: www.cornwall.gov.uk Telephone: 0300 1234 101

- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London SW1P 3BT Telephone: 0870 000 2288
  Website: www.education.gov.uk email: info@education.gsi.gov.uk

Attendance is not collected for pupils under 5 at Early Years Settings or Maintained Schools