
# Ysgol Bro Carmel

# E-Safety and Online Learning Policy

# 2024 – 2025

**Date Adopted: Autumn 2024**

**Date of Review: Autumn 2025**

**Committee: FGB**

**Social Media Policy and Declaration**

The E-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 E-Safety or incidents that have taken place.

Should serious E-Safety incidents take place, the following external persons / agencies should be informed: LA Safeguarding Officer – ICT Support (if needed) Social Services

The school will monitor the impact of the policy using:

Logs of reported incidents

Monitoring logs of internet activity (including sites visited) (On-site Technical Support)

Internal monitoring data for network activity (On-site Technical Support Person)

Surveys / questionnaires of pupils, parents / carers, staff

**Scope of the Policy**

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix).

The school will deal with such incidents within this policy in addition to the associated safeguarding (including our prevent strategy+), behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-Safety behaviour that take place out of school.

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school:

**Governors**:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports. A member of the Governing Body will taken on the role of E-Safety. The role of the E-Safety Governor will include:

- ✓ regular meetings with the member(s) of SLT responsible for E-Safety
- ✓ regular monitoring of E-Safety incident logs
- ✓ regular monitoring of filtering / change control logs
- ✓ reporting to relevant Governors meetings

**Headteacher and Senior Leaders:**

The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community; the day to day responsibility for E-Safety will be delegated to all staff.

The Headteacher and the other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff. (see flowchart on dealing with E-Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR).

The Headteacher / Senior Leaders are responsible for ensuring that other relevant staff receive suitable training to enable them to carry out their E-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 E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

**E-Safety Lead:**

- ✓ takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents.
- ✓ ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place this will include online networking and radicalisation
- ✓ provides training and advice for staff
- ✓ liaises with the Local Authority if necessary
- ✓ liaises with technical support staff
- ✓ receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments,
- ✓ meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering control logs.
- ✓ attends relevant training and committee of Governors meetings
- ✓ reports regularly to other members of the Senior Leadership Team

**Network Manager / Technical staff:**

The Network Manager / Technical Staff for Computing are responsible for ensuring:

- ✓ that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- ✓ that the school meets required E-Safety technical requirements and any statutory guidance that may apply.
- ✓ that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed where and when appropriate
- ✓ the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (currently the responsibility of the LA)
- ✓ that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant.
- ✓ that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; E-Safety Lead for investigation / action / sanction. The approach needs to be evaluated regularly in light of new developments and methods.
- ✓ that monitoring software / systems are implemented and updated as agreed in school policies this will include online networking and radicalisation.

**Teaching and Support Staff**

are responsible for ensuring that:

- ✓ they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- ✓ they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- ✓ they report any suspected misuse or problem to the Headteacher / Senior Leader; E-Safety Lead 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
- ✓ E-Safety issues are embedded in all aspects of the curriculum and other activities
- ✓ pupils understand and follow the E-Safety and acceptable use policies
- ✓ 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. This includes the Prevent Strategy.
- ✓ 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.

**Designated Safeguarding Leads**

should be trained in E-Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

**Pupils**:

- ✓ are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
- ✓ have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- ✓ need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- ✓ will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- ✓ should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- ✓ will experience E-Safety training as part of their curriculum each year.

**Parents / Carers**

- ✓ Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Seesaw and information about national / local E-Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:
- ✓ digital and video images taken at school events
- ✓ their children's personal devices in the school (where this is allowed)

**Students/Work Experience/Volunteers/Community Users**

Students/Work Experience/Volunteers/Community Users who access school systems / website / Seesaw as part of the wider school provision will be expected to sign a Community User AUA (Acceptable Use Agreement) before being provided with access to school systems.

**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 E-Safety is therefore an essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience.

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

A planned E-Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited

Key E-Safety messages should be reinforced as part of a planned programme of assemblies and class council 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 helped to understand the need for the pupil Acceptable Use Agreement 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 and insist in the use of safe search engines.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics 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 E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- ✓ Curriculum activities
- ✓ Letters, newsletters, website, Email, SMS
- ✓ Parents / Carers evenings / sessions
- ✓ High profile events / campaigns e.g. Safer Internet Day
- ✓ Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see school website and appendix for further links / resources)

**Education – The Wider Community**

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

- ✓ Providing family learning courses in use of new digital technologies, digital literacy and E-Safety
- ✓ E-Safety messages targeted towards grandparents and other relatives as well as parents.
- ✓ The school website will provide E-Safety information for the wider community
- ✓ Where and when appropriate supporting community groups e.g. Early Years Settings, Child-minders, youth / sports / voluntary groups to enhance their E-Safety provision.

**Education & Training – Staff / Volunteers**

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

- ✓ A planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. It is expected that some staff will identify E-Safety as a training need within the performance management process.
- ✓ All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements.
- ✓ The E-Safety Lead will receive regular updates through attendance at external training events (e.g. from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- ✓ This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- ✓ The E-Safety Lead will provide advice / guidance / training to individuals as required.

**Training – Governors**

- ✓ Governors should take part in E-Safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / E-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 / or other relevant organisation.
- ✓ Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

**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 previous sections will be effective in carrying out their E-Safety responsibilities:

- ✓ School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- ✓ There will be regular reviews and audits of the safety and security of school technical systems.
- ✓ Servers, wireless systems and cabling must be securely located and physical access restricted (Server Room).
- ✓ All users will have clearly defined access rights to school technical systems and devices.
- ✓ All users will be provided with a username and secure password by in house technical support who will keep an up-to-date record of users and their usernames. Staff users are responsible for the security of their username and password and will be required to change their password where and when appropriate
- ✓ The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and secured.
- ✓ The School Business Manager in liaison with the technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- ✓ Internet access is filtered for all users. Illegal content is filtered by the broadband/filtering provider.
- ✓ School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. (see appendix)
- ✓ An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- ✓ Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- ✓ An agreed protocol is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- ✓ An agreed protocol is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- ✓ An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

**Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for Cyber Bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential 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 e.g. on social networking sites.
- ✓ In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images
- ✓ 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 of staff should not be used for such purposes.
- ✓ Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- ✓ Pupils must not take, use, share, publish or distribute images of others without their permission.
- ✓ Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- ✓ Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- ✓ Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (covered as part of the AUA signed by parents or carers at the start of Foundation Stage or when the child joins the school - see Parents / Carers Acceptable Use Agreement in the appendix)

**Pupil Acceptable Use Agreement Pupils**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- ✓ that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- ✓ that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users

**Ysgol Bro Carmel**

- ★ I will only access computing equipment when a trusted adult has given me permission and is present.
- ★ I will not deliberately look for, save or send anything that could make others upset.
- ★ I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- ★ I will keep my username and password secure; this includes not sharing it with others.
- ★ I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- ★ I will always use my own username and password to access the school network and subscription services.
- ★ In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- ★ I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- ★ I will use all communication tools such as email and blogs carefully.
- ★ I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- ★ Before I share, post or reply to anything online, I will T.H.I.N.K.


- ★ I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

**Please sign below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access may not be granted to school systems and devices.**

*Signed (child):* _____

*Signed (parent)*: _____

# Pupil Acceptable Use Agreement for KS1

## Ysgol Bro Carmel

**This is how we stay safe when we use computers:**

- ★ I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- ★ I only open activities that an adult has told or allowed me to use.
- ★ I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- ★ I keep my passwords safe and will never use someone else's.
- ★ I know personal information such as my address and birthday should never be shared online.
- ★ I know I must never communicate with strangers online.
- ★ I am always polite when I post to our blogs, use our email and other communication too.

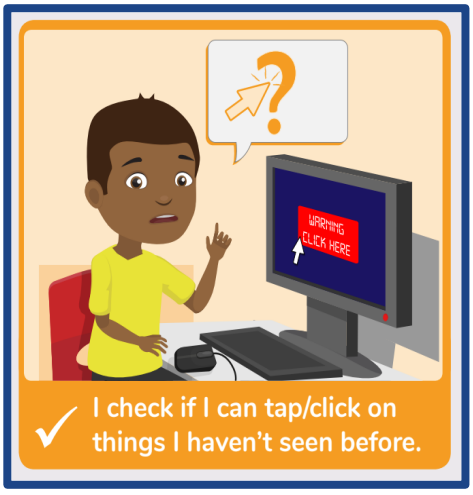
*My Name (child):* _____

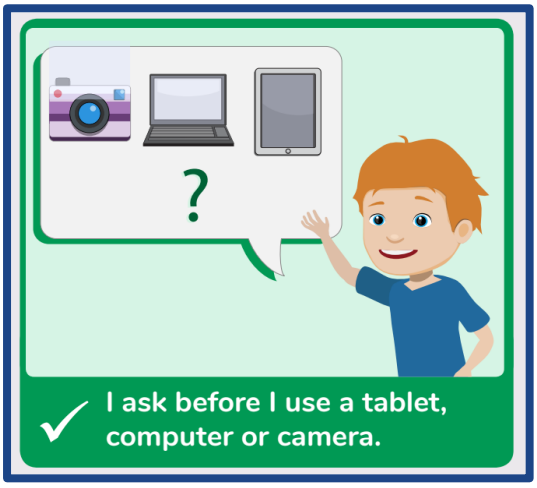
*Signed (parent)*: _____

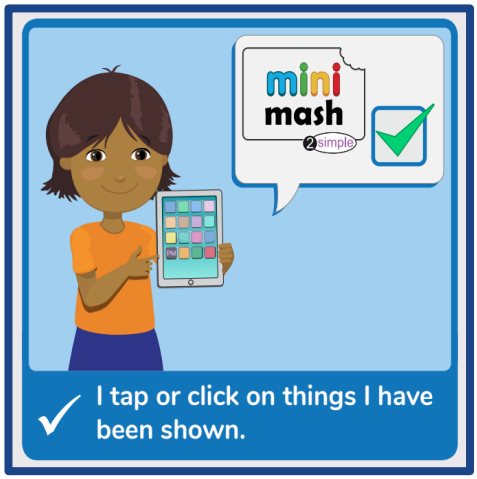
# Pupil Acceptable Use Agreement for EYFS

## Ysgol Bro Carmel

## This is how we stay safe when we use computers:


*My Name (child):*

_____

*Signed (parent)*:

_____

**Staff and Volunteer Acceptable Use Agreement**

**Ysgol Bro Carmel**

**School Policy**

New and constantly changing technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- ✓ that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- ✓ that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- ✓ that staff are protected from potential risk in their use of ICT in their everyday work.

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

**Acceptable Use Policy Agreement**

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

For my professional and personal safety:

- ✓ I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- ✓ I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- ✓ I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- ✓ I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- ✓ I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- ✓ I will be professional in my communications and actions when using school ICT systems:
- ✓ I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- ✓ I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- ✓ I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- ✓ I will only use chat and social networking sites in school in accordance with the school's policies.
- ✓ I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- ✓ I will not engage in any online activity that may compromise my professional responsibilities.

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

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

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

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

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

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

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

Full Name: …… Signed:……..Date: ……..