

Mountjoy School

Online Safety Policy

December 2023



This is a Dorset Council Policy
Reviewed by: Senior Leadership Team

Date: December 2023
Date of next review: December 2024

This policy must be read in conjunction with the following policies:

- **Child Protection and Safeguarding Policy**
- **Behaviour Policy**
- **Staff Disciplinary Procedures**
- **Data protection policy and Privacy Notices**
- **Complaints Procedure**
- **Social Networking Policy**

This policy sets out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of Online Safety;
- work to empower the school community to use the internet as an essential tool for life-long learning.

This policy is used in conjunction with other school policies.

What is Online Safety?

Online Safety refers to child protection and safeguarding of both children and adults in the digital world. It is about learning to understand and use technologies in a safe, positive way. It is also about supporting children and adults to develop safe online behaviours (both in and out of school).

Risks to children who use the internet include:

- Exposure to inappropriate materials, for example, pornographic pictures and videos
- Physical danger and sexual abuse, for example, through 'grooming' by paedophiles
- Obsessive use of the internet and ICT, for example, addiction to video games
- Cyber bullying – persistent bullying through the digital medium
- Inappropriate or illegal behaviour, for example, exposure to hate mail or offensive images
- Copyright infringement, for example, the illegal sharing of music, pictures, video or documents

There are also risks to staff that use the internet.

Online Safety is largely concerned with internet communications. The internet is accessible from computers, laptops, tablets, mobile phones, games consoles and other devices like the iPad, iPod Touch and internet connected TV. Other communication technologies, such as texting and phone calls, are also covered by the term 'Online Safety'.

Scope of Policy

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

The school will manage Online Safety, as described within this policy and the associated Behaviour Policy, and will inform parents and carers of known incidents of inappropriate Online Safety behaviour that take place in and out of school.

This policy should be read in conjunction with the school's Acceptable Use Policy (AUP) agreement.

Roles and Responsibilities

The head teacher is responsible for ensuring the safety (including Online Safety) of all members of the school community, though the day to day responsibility for Online Safety can be delegated.

The Online Safety leader will work with the designated child protection co-ordinator and will have overview of the serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber bullying.

Role	Responsibility
Governors	<ul style="list-style-type: none">• Approve and review the effectiveness of the Online Safety Policy• Online Safety responsibility will be with the child protection governor
Head Teacher and Senior Leaders	<ul style="list-style-type: none">• Ensure that all staff receive suitable CPD to carry out their Online Safety roles• Create a culture where staff and learners feel able to report incidents• Ensure that there is a system in place for monitoring Online Safety• Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff or pupil• Inform the local authority about any serious Online Safety issues• Ensure that the school infrastructure/network is as safe and secure as possible (through Online Safety lead report to governors)• Ensure that policies and procedures approved within this policy are implemented

Online Safety Leader	<ul style="list-style-type: none"> • In conjunction with head teacher log, manage and inform others of Online Safety incidents • Lead the establishment and review of Online Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to Online Safety • Provide and/or broker training and advice for staff • Attend updates and liaise with the LA Online Safety staff and technical staff • Meet with Senior Leadership Team and Online Safety governor when necessary to discuss incidents and developments • Co-ordinate work with the school's designated child protection co-ordinator
Teaching and Support Staff	<ul style="list-style-type: none"> • Participate in any training and awareness raising sessions • Read, understand and sign the staff AUP • Act in accordance with the AUP and Online Safety Policy • Report any suspected misuse or problems to the Online Safety leader • Monitor ICT activity in lessons, extra-curricular and extended school activities • Ensure that Online Safety is taught as part of the curriculum
Pupils	<ul style="list-style-type: none"> • Participate in Online Safety activities
Parents and Carers	<ul style="list-style-type: none"> • To sign the home school agreement, thereby endorsing their understanding of this policy • Discuss Online Safety issues with their child(ren) and monitor their home use of ICT systems (including mobile phones and games devices) and the internet • Access the school website • Inform the head teacher of any Online Safety issues that relate to the school

Technical Support Provider	<ul style="list-style-type: none"> • Ensure the school’s ICT infrastructure is as secure as possible • Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with Online Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the Online Safety leader for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows)
-----------------------------------	---

Education of pupils

A progressive, planned Online Safety education programme is currently starting for some children in all stages, and is regularly reviewed.

- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.
- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches. Staff pre-check any searches.
- Pupils are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information.

Education and information for parents and carers

Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. The school supports parents and carers to do this:

- through the use of the Family Liaison Officer;
- by raising awareness through activities planned by pupils;
- through endorsing its message in the whole school agreement;

- through the school website links to online Online Safety sites providing guidance for parents and carers www.ceop.police.uk www.thinkuknow.co.uk www.childnet.com and www.kidsmart.org.uk

Training of Staff and Governors

There is a planned programme of Online Safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUP. This includes:

- an annual audit of the Online Safety training needs of **all** staff;
- **all** new staff required to sign AUP and read this policy;
- this Online Safety Policy and its updates being shared with staff;
- the Online Safety leader providing guidance and training as required to individuals and seeking LA support on issues;
- UK Safer Internet Centre helpline 0844 381 4772 is displayed on the staff notice board.

Cyber bullying

Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- The school will follow procedures in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying reported to the school will be recorded.
- The school will follow procedures to investigate incidents or allegations of cyber bullying.
- Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.
- The school will take steps, where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
- Pupils, staff and parents and carers will be required to work with the school to support the approach to cyber bullying and the school's Online Safety ethos.
- Sanctions for those involved in cyber bullying will follow those for other bullying incidents and may include:
 - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses, or is unable, to delete content.
 - Internet access may be suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance with the school's Anti-bullying, Behaviour Policy or staff AUP.

- Parents and carers of pupils will be informed.
- The police will be contacted if a criminal offence is suspected.

Technical Infrastructure

The person(s) responsible for the school's technical support will sign the staff AUP.

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- The School ICT systems are managed in ways that ensure that the school meets Online Safety technical requirements.
- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, etc from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:
 - the downloading of executable files by users
 - the installing of programmes on school devices, unless permission is given by the technical support provider or ICT co-ordinator
 - the use of removable media (eg memory sticks) by users on school devices
 - the installation of up to date virus software
- Access to the school network and internet will be controlled with regard to:
 - users having clearly defined access rights to school ICT systems through group policies
 - users, where appropriate, being made aware that they are responsible for the security of their username and password and must not allow other users to access the systems using their log on details
 - users must immediately report any suspicion or evidence that there has been a breach of security
 - an agreed process being in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) on to the school system. All "guests" must sign the staff AUP and are made aware of this Online Safety Policy
- The internet feed will be controlled with regard to
 - the school maintaining a managed filtering service provided by an educational provider
 - the school monitoring internet use
 - any filtering issues being reported immediately to SWGfL helpline

- The ICT system of the school will be monitored with regard to:
 - the school ICT technical support regularly monitoring and recording the activity of users on the school ICT systems
 - Online Safety incidents being documented and reported immediately to the Online Safety leader who will arrange for these to be dealt with immediately in accordance with the AUP

Data Protection

The SWGfL Data Protection Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

The school will:

- 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
- ensure that users are properly “logged-off” at the end of any session in which they are accessing personal data
- make sure data is deleted from the device or SLP once it has been transferred or its use is complete

Use of digital and video images

Staff, governors, volunteers and work placement/work experience students must be aware of their responsibilities and limitations when using digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers and to provide information about the school on the website. The school will:

- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Allow staff to take images on school photographic and video equipment only, to support educational aims, but follow guidance in the AUP concerning the sharing, distribution and publication of those images.
- Make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Make sure that pupils’ full names will not be used anywhere on the school website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images or videos of pupils are electronically published.

- Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use.

Communication (including use of Social Media)

A wide range of communications technologies have the potential to enhance learning. The school will:

with respect to email

Staff, governors, volunteers and work placement/work experience students must be aware of their responsibilities and limitations when using email

- Ensure that all school business will use the official school email service.
- Make users aware that email communications may be monitored.
- Users to report an incident of receipt of an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Teach pupils about email safety issues through the scheme of work.
- Ensure that personal information is not sent via email.
- Only publish official staff email addresses.

with respect to social media

Staff, governors, volunteers, supply and work placement/work experience students must be aware of their responsibilities and limitations when using social media

- Control access to social media and social networking sites.
- Provide staff with the tools to risk assess sites before use and check the site's terms and conditions to ensure the site is age appropriate.

with respect to personal publishing

- Teach pupils via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Register concerns regarding pupils' use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites.
- Outline safe and professional behaviour.

with respect to mobile phones

Staff, governors, volunteers, supply and work placement/work experience students must be aware of their responsibilities and limitations when using mobile phones

- **Are NOT PERMITTED** to take photographs or video of pupils on their personal mobile phone or video camera.
- **Are NOT PERMITTED to use their personal mobile phone or have it on their person during pupil contact time** and that it should be stored ideally in a locked cupboard during working hours. The ONLY exception to this rule is for offsite visits, where the restricted use of personal mobiles phones will be permitted in accordance with the school's Offsite Visits and Activities Policy.
- Are only permitted to use their personal mobile phone during their staff breaks and to avoid interfering with other staff on breaks, will make calls from outside the school buildings and out of sight of pupils.
- Provide a business mobile phone for activities that require them.

Allow pupils to bring mobile phones into school with the specific agreement of the head teacher.

The following table shows how the school considers how all these methods of communication should be used.

Communication Technologies Also see Social Networking Policy	Staff & other adults			
	Allowed	Allowed at specified times	Allowed for authorised selected staff	Not allowed
Personal mobile phones may be brought to school	✓			
Use of personal mobile phones in lessons		✓		
Use of personal mobile phones in social time	✓			
Taking photos on personal mobile phones or other camera personal devices				✓
Use of personal email addresses in school, or on school network		✓		
Use of school email for personal emails				✓
Use of personal mobile phones to access chat rooms / facilities				✓
Use of personal mobile phones to access instant messaging				✓
Use of personal mobile phones to access social networking sites				✓
Use of personal mobile phones to access blogs				✓
Use of personal mobile phones to access Twitter				✓
Use of personal mobile phones to access YouTube				✓

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the Online Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate material.

However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the police.

Reporting and Response to Incidents

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyber bullying, illegal content, etc).
- The Online Safety leader will record all reported incidents and actions taken in the school Online Safety incident log and in any other relevant areas, eg bullying or child protection log.
- The designated child protection co-ordinator will be informed of any Online Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.
- The school will manage Online Safety incidents in accordance with the school Behaviour Policy.
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Dorset Children Safeguarding Team and escalate the concern to the police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Schools Adviser, Local Authority Designated Officer (LADO) or Senior ICT Adviser.

The police, and where necessary the Prevent lead for the local authority, will be informed where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material
- extremist material

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures will be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- using school systems to run a private business
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and the school
- 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 or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

In addition, the following indicates school policy on these uses of the internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
On-line gaming (educational)				√
On-line gaming (non-educational)				√
On-line gambling				√
On-line shopping / commerce		√		
File sharing (using p2p networks)				√

Sanctions for Misuse: Pupils

Schools should populate the grid below marking appropriate possible sanctions.

Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore, ticks may appear in more than one column.

The ticks in place are actions which must be followed.

Incidents:	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).					✓		✓	
Unauthorised use of non-educational sites during lessons		✓					✓	
Unauthorised use of mobile phone / digital camera / other handheld device		✓			✓		✓	
Unauthorised use of social networking / instant messaging / personal email		✓			✓		✓	
Unauthorised downloading or uploading of files		✓			✓		✓	
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		✓			✓		✓	

Sanctions/Actions: Staff

Schools should populate the grid below marking appropriate possible sanctions.

Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore, marks may appear in more than one column.

The marks in place are actions which must be followed.

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(P)	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	L P	✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓	✓		✓	✓	✓	✓
Unauthorised downloading or uploading of files		✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓			✓	✓	✓	✓
Careless use of personal data eg holding or transferring data in an insecure manner		✓	✓		✓	✓	✓	✓
Deliberate actions to breach data protection or network security rules		✓	✓		✓	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓					✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff		✓	✓			✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners		✓	✓	L		✓	✓	✓
Breach of the school Online Safety policies in relation to communication with learners		✓	✓	L		✓	✓	✓
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils		✓	✓	L		✓	✓	✓
Actions which could compromise the staff member's professional standing		✓	✓			✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓			✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓			✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓	L		✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	L		✓	✓	✓
Breaching copyright or licensing regulations		✓						✓
Continued infringements of the above, following previous warnings or sanctions		✓				✓		✓

Online Safety: Staff, Supply, Volunteer and Work Experience Students – Acceptable Use Policy

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

This Acceptable Use Policy is intended to ensure that:

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

The school will try to ensure that staff, supply and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff, supply 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 students 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 Online Safety in my work with young people.

Use of Social Media

The school makes planned and managed use of some social media tools, including YouTube and Vimeo. Content can only be uploaded by staff account holders. The sites may be used by pupils as part of a managed learning activity. The school expects all staff members and students to access these materials appropriately and not use them to cause offence or harm.

For my professional and personal safety:

- I understand that the school can 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 etc) 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 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 (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school
- I will only communicate with students/parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line 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 personal hand held/external 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 open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs
- 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 programs of software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings
- I will not attempt to use my personal pen drive in any school machine/device
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school
- I understand that if I fail to comply with the 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

This policy should be read in conjunction with the Single Equality Policy. The general equality duty requires that, in the exercise of their functions, schools must have due regard to the need to eliminate unlawful discrimination, harassment, victimisation and other conduct prohibited by the Equality Act 2010. This school endeavours to advance equality of opportunity and foster good relations for all.

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.

Staff/Supply / Volunteer/
Work Experience Student
Name

Signed

Date

Parent/Carer Acceptable Use Agreement

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

This Acceptable Use Policy is intended to ensure:

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

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care. Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name

Pupil Name

As the parent/carers of the above pupil, I give permission for my son/daughter to have access to the internet and to ICT systems in school.

I understand that the school has discussed the Acceptable Use Agreement with my son/daughter and that they have received, or will receive, Online Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies. I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

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

Signed

Date

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

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

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

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

Digital/Video Images Permission Form

Parent/Carers Name

Pupil Name

As the parent/carer of the above pupil, I agree to the school taking and using digital/video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes/No






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

Yes/No

Signed



Acceptable Use Policy






This is how we stay safe




when we use the computer










 I will ask an adult if I want to use the computer.
























 I will only do what an adult has told me to do.











 I will take care of the computer equipment.










 I will ask for help from a member of staff if I am







 not sure what to do or if I have done something wrong.

 I  will tell  an adult  if I  see something that

 upsets  me  on the computer.

 I  know that if  I  break these rules  I may  not be

 allowed to use a  computer.

 My  name is

 and  my  signature is

 The date is

Online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	Date:
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school’s acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school’s ICT systems?	
Are you familiar with the school’s approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

