



Learning for Life

Online Safety and Acceptable Use Policy

Policy Name	Online Safety and Acceptable Use Policy
Governors responsible for review	TBC
Date Approved By Committee	TBC
Amended to include updates	02.02.2024
Review Cycle	Annually
Statutory/Recommended/Optional	Statutory

Our Mission Statement

Our Mission statement is based on the values of empathy and respect for all, diversity, integrity, faith and being proud of who you are.

'Nurturing the individual as part of a caring and sharing community'

AIMS

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and

Online Safety and Acceptable Use Policy

non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

KEY SCHOOL STAFF

Details of the schools' Designated Safeguarding Lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions. The DSL AND THE Computing Lead are responsible for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently.
- Working with the ICT technician, the school business manager and other staff, as necessary, to address any online safety issues or incidents.
 - Managing all online safety issues and incidents in line with the school policy. Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with policy.
- Updating and delivering staff training on online safety, when necessary
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board

DSL – Mrs Nuala Heslop

Computing Lead – Mr Simon Kinder

Deputy DSLs – Mrs Julie Lomas and Mrs Tracy Whealing

IT SUPPORT

- Ensuring that appropriate security protection procedures are in place which are reviewed and updated on a regular basis to assess effectiveness and, with the safeguarding team, ensure that pupils are kept safe from potentially harmful and inappropriate content and contact online while at school including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are up to date.
- Working with the safeguarding team to test the filtering systems on a termly basis.
- Ensuring systems are in place that block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files.
- Record 'online alerts' and associated actions. Contact RM if required.

The Managed Service provider is RM

ALL STAFF AND VOLUNTEERS

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the schools' ICT systems and the internet (appendix 3), and ensuring that pupils follow the schools' terms on acceptable use (appendices 1 and 2)
- Working with the DSL/DDSLs to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
 - Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school anti-bullying policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

PARENTS

Parents are expected to:

- Notify the Headteacher/DSL of any concerns or queries regarding this policy.
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
 - What are the issues? – UK Safer Internet Centre
 - Hot topics – Childnet International
 - Parent resources sheet – Childnet International

Online Safety and Acceptable Use Policy

There are also a selection of parental resources available on the school website

- Support their children's appropriate use of social media and online behaviour, being aware of age restrictions on certain apps;
- Facebook 13 years +
- Instagram 13years +
- TIKTOK 13 years +
- Snap Chat 13 years +
- WhatsApp 16 years +
- YouTube 18 years but 13 years with permission of parent.
- Discord 13years +

VISITORS AND MEMBERS OF THE COMMUNITY

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum: The text below is taken from the National Curriculum computing programmes of study. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools must teach: Relationships education and health education in primary schools

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact. By the end of primary school, pupils will know:
 - That people sometimes behave differently online, including by pretending to be someone they are not.
 - That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
 - The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.

Online Safety and Acceptable Use Policy

- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
 - How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
- The safe use of social media and the internet will also be covered in other subjects where relevant.
 - Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

EDUCATING PARENTS ABOUT ONLINE SAFETY

The schools will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers via the schools' website. Online safety is covered in PHSE lessons, computing lessons and will also be covered during Safer Internet Day and online safety workshops. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher. Concerns or queries about this policy can be raised with Headteacher/DSL/DSLs. Opportunities at Parent Conferences to provide parents with online safety information.

CYBER-BULLYING

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school anti-bullying policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Class teachers will discuss cyber-bullying with their class. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. The school also sends information/leaflets on cyber-bullying to parents (also available on the school website) so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying policy.

Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The

Online Safety and Acceptable Use Policy

DSL/DDSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

EXAMINING ELECTRONIC DEVICES

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or

Disrupt teaching, and/or

Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL/DDSL or other member of the senior leadership team to decide whether they should:

Delete the material, or

Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or

Report it to the police** * If a staff member believes a device may contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next.

The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents, staff, volunteers and governors are expected to read this policy regarding the acceptable use of the schools' ICT systems and the internet (Visitors . Use of the schools' internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites

Online Safety and Acceptable Use Policy

visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

STAFF USING WORK DEVICES OUTSIDE OF SCHOOL

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends. Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way which would violate the schools' terms of acceptable use. If staff have any concerns over the security of their device, they must seek advice immediately.

TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, ebulletins and staff meetings). By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term. The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if










Online Safety and Acceptable Use Policy

applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

COMMUNICATION METHOD OR DEVICE


The following table shows the school's policy on the use of communication devices and methods (during the school day)

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

Communication method or device	Staff & other adults				Students/Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Mobile phones may be brought to school	<input checked="" type="checkbox"/>							
Use of mobile phones in lessons								<input checked="" type="checkbox"/>
Use of mobile phones in social time	<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>
Taking photos on mobile phones or other camera devices								<input checked="" type="checkbox"/>
Use of personal email addresses in school, or on school network				<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Use of chat rooms / facilities				<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Use of instant messaging				<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Use of social networking sites				<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Use of blogs								

Online Safety and Acceptable Use Policy

On-line shopping								
------------------	--	---	--	--	--	--	--	---

 This table shows when some of the methods detailed above may be allowed:

Communication method or device	Circumstances when these may be allowed	
	Staff & other adults	Pupils
Use of Mobile phones in social time	During breaks times, lunchtimes (if not on duty) and after school	Not allowed
Taking photos on personal mobile phones or other camera devices	If school device is not available. All photos must be uploaded and deleted from the device as soon as possible.	If staff permission is given during a lesson to record activities/progress
Using mobile phones during lessons	<p>If school device is not available. All photos must be uploaded and deleted from the device as soon as possible.</p> <p>During a school trip to contact other staff/aduls.</p>	Not allowed
Use of blogs	Blogs can be used by teaching staff	Under the supervision of a member of staff
On-line shopping	There may be a need to purchase resources online.	Not allowed

INCIDENT MANAGEMENT

Online Safety and Acceptable Use Policy

Infringements – Pupils	Sanctions
<p>*The following are provided for exemplification only.</p>	
Category A	
Use of non-educational sites during lessons	<ul style="list-style-type: none"> • Referred to class teacher • Refer to DSL if deemed a safeguarding issue
Category B	
Continued use of non-educational sites during lessons after being warned.	<ul style="list-style-type: none"> • Refer to class teacher, then DSL Next steps/consequences agreed by both. • If deemed more serious, consult with Headteacher. • Parents informed if deemed necessary.
Use of file sharing software e.g. Napster, Vanbasco, Bit Torrent, LiveWire, etc	
Accidentally corrupting or destroying others' data without notifying a member of staff	
Accidentally accessing offensive material and not logging off or notifying a member of staff	
Category C	
Deliberately corrupting or destroying someone's data, violating privacy of others.	<ul style="list-style-type: none"> • Refer to class teacher, then DSL – next steps agreed • If deemed more serious, consult with Headteacher. • Parents Informed • Removal of internet access rights for a period of time • Removal of equipment • Investigate as per Safeguarding policy if applicable • If inappropriate web material is accessed then report to RM Services
Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)	
Deliberately trying to access offensive, extremist or pornographic material	
Any purchasing or ordering of items over the internet	
Category D	
Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned	<ul style="list-style-type: none"> • Refer to class teacher, then DSL – next steps agreed • If deemed more serious, consult with Headteacher. • Parents Informed • Removal of internet access rights for a period of time • Removal of equipment • Investigate as per Safeguarding/Child Protection policy
Deliberately accessing, downloading and disseminating any material deemed offensive, extremist, obscene, defamatory, racist, homophobic or violent	
Receipt of transmission of material that infringes the	

Online Safety and Acceptable Use Policy

copyright of another person or infringes the conditions of the Data Protection Act.	<p>if applicable</p> <ul style="list-style-type: none"> • If appropriate web material is accessed then report to RM Services • Report to Police • Refer to Anti-bullying Policy, Safeguarding Policy <p>Other safeguarding actions</p> <ul style="list-style-type: none"> ✓ Secure and preserve any evidence
Bringing the school name into disrepute	

Infringements – Staff/Adults	Sanctions
<p>*The following are provided for exemplification only.</p>	
Category A	
Excessive use of internet for personal activities not related to professional development e.g. online shopping, personal email etc	<ul style="list-style-type: none"> • Refer to DSL • Warning given and recorded • <u>Multiple</u> category A infringement will escalate the severity of the action (will move to category B sanction)
Breaching copyright or license e.g. installing unlicensed software onto the network	
Use of mobile phone during teaching time (for other than professional use – see Communication and devices section)	
Category B	<ul style="list-style-type: none"> • Referred to Headteacher and DSL • School disciplinary procedures followed • Report to HR (if deemed necessary) • Report to Police if appropriate <p>LA Safeguarding Officer – Roisin Rafferty LA IT Manager Terry Walsh</p>
Serious misuse of , or deliberate damage to, any school computer, hardware or software	
Any deliberate attempt to breach data protection or computer or computer security settings	
Deliberately accessing, downloading and disseminating any material deemed offensive, extremist, obscene, defamatory, racist, homophobic or violent	
Receipt of transmission of material that infringes the copyright of another person or infringes the conditions of the	

Online Safety and Acceptable Use Policy

Data Protection Act.	
Bringing the school name into disrepute	

LINKS WITH OTHER POLICIES

This online safety policy is linked to our:
Child Protection and Safeguarding Policy
Anti-Bullying Policy
Staff Disciplinary Procedures
Data Protection Policy and Privacy Notices
Complaints Procedures

FURTHER INFORMATION AND SUPPORT

For a glossary of terms used in this documents:

<http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf>

For e-Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People;

<http://www.salford.gov.uk/d/e-Safety-Practice-Guidance.pdf>

R u cyber safe?

E-safety tips about how to stay safe online:

<http://www.salford.gov.uk/rucybersafe.htm>

Pupil Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I may have access to the school network/internet taken away from me, my parents/carers might be informed, I may have to explain my actions to the school leadership team, or in the event of illegal activities, to the police.

I have read and understand the above and agree to follow these guidelines when:

- I use the school IT systems and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, website etc

Staff, Volunteer and Community User Acceptable Use Policy Agreement

School Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, volunteers and community users 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, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

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

Online Safety and Acceptable Use Policy

- 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. 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 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 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 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 in line with the School's Online Safety Policy 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.

Online Safety and Acceptable Use Policy

- 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 programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, extremist material, 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.
- 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/Local Authority Personal Data Policy. Where personal data is transferred outside the secure school network, it must be done so securely.
- 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).

Staff, Volunteer and Community User Acceptable Use Agreement Form

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 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