Rainow Primary School

Caring, Learning, Achieving.

e Safety Policy

Members of staff responsible:	**Mr Norris / Mr Trueman (SL)**
Date approved by Governors:	**Summer 2024**
Date to be reviewed:	**Summer 2027**

1. 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 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

2. 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.
- 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.

3. Roles and responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).
- Ensure that online safety is a running and inter-related theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

- Providing termly reports on online safety in school to the headteacher and/or governing board.

3.3 The Designated Safeguarding Lead (DSL) with Support from the Computing Lead

Details of the school's designated safeguarding lead (DSL) deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, Computing Subject Leader, ICT 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 child protection policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Supporting the Headteacher to provide termly reports to the governing board.

This list is not intended to be exhaustive.

3.4 ICT support / manager

We employ ICT support / management from Cheshire East Traded Services. They visit the school for one day every fortnight to ensure school ICT systems are safe, updated and reliable. They also provide ad hoc phone and email support.

ICT support / manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure 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 updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on at least a fortnightly basis (They will conduct ore frequent checks if instructed by the school).
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged 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 behaviour policy.

This list is not intended to be exhaustive.

3.5 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 school's ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendix 2).
- Working with the DSL to ensure that any online safety incidents are logged 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 behaviour 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'.

This list is not intended to be exhaustive.

3.6 Pupils

Pupils are expected to:

- Understand and agree to the Pupil Acceptable Use Policy Agreements (Appendix 2a and 2b). These will be reminded to the children at the beginning of every academic year, as a minimum, and also as and when they are relevant.
- Keep their personal passwords safe and not share them with other pupils.
- Deny access to unknown individuals and to block unwanted communications.
- Only use approved e-mail accounts on the school system.
- Tell a teacher immediately if they receive offensive messages or see inappropriate materials.
- Ask permission from the supervising teacher before making or answering a voice or video conference.
- Never give out personal details of any kind which may identify them or their location.
- Invite known friends only and deny access to others when using social networking sites and or digital learning platforms.
- Not arrange to meet anyone without specific permission.
- The Digital Leaders, selected pupils from KS2 who champion, support and help lead Computing in school, will seek to model and promote good internet use.

This list is not intended to be exhaustive. Please see Appendix 2 – 'Pupil Acceptable Use Policy'

3.7 Parents

Parents are expected to:

- Read, understand and agree to the Parent / Carer Acceptable Use Policy Agreement (Appendix 3). This will be sent to families at the beginning of their child's schooling and reminded to them annually.
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 2).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre
Help, advice and resources for parents and carers – Childnet International

3.7 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. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Teaching and Learning / Online Safety

4.1 Curriculum

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

Relationships Education and **Computing**

In **Key Stage 1 Relationships Education,** 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.

In **Key Stage 1 Computing,** 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.

In **Key Stage 2 Relationships Education, pupils** 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.
  - 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.

Pupils in **Key Stage 2 Computing, pupils** will be taught to:

- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

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.

4.2 Rainow School Network / Web content filtering and monitoring

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] risks from the school's or college's IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Our school meets these requirements in the following ways:

- Our safe and secure broadband is provided by Schools Broadband, a specialist Education Internet Service Provider (ISP).
- Schools Broadband provide effective management of content filtering as part of the school's subscription. The content filtering system used is Netsweeper, which facilitates restrictive settings for different user profiles.
- The school's internet access will be employed expressly for education and will include age-appropriate content filtering.
- The school will work with the LA to ensure systems to protect pupils are reviewed and improved. The content filtering system used is Netsweeper, which facilitate restrictive settings for different user profiles.
- The DSLs, Computing Lead and admin staff receive a Daily Online Safeguarding Report from Schools Broadband. This report covers the following areas:
    - Illegal online content
    - Inappropriate online content
    - Copyright infringement
    - Security-related risks
    - Denied keywords
    - Top 10 search keywords

  Any evidence of unsafe and/or inappropriate online behaviour found on the Daily Online Safeguarding Report will be investigated and dealt with by the DSL / Computing Lead and Headteacher.
- If staff or pupils discover an unsuitable site, it must be reported to the class teacher, Computing Subject Leader, DSLs or Headteacher.
- Virus protection will be installed on every computer and will be set to update automatically in real time.
- IP video conferencing should use the educational broadband network to ensure quality of service and security.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Arbor app. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings. The school will let parents know:

- What systems the school uses to filter and monitor online use.

- What their children are being asked to do online, who from the school (if anyone) their child will be interacting with online.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 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 schools' behaviour and anti-bullying policies.)

6.2 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.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also signposts information/leaflets on cyber-bullying to parents 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 behaviour and anti-bullying policies. 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 DSL 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.

6.3 Examining electronic devices

It is school policy that no child at Rainow Primary School will be allowed to bring in personal electronic devices (usually mobile phones) unless they are needed to contact parents on journeys to and from school (usually children in Upper Key Stage 2). In this instance, the arrangement will have been made between school and the family, and the device will remain locked away in the school office until it is needed.

Although unlikely, the headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.
- Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from an authorised member of staff.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident 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

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.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may not bring personal mobile devices into school unless a member of the Leadership Team has granted permission. **(also see 6.3)**

9. Staff using work devices outside 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 (this will be done and kept updated by ICT support / manager).
- Keeping operating systems up to date by always installing the latest updates, (this will be done and kept updated by ICT support / manager).

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from ICT support / manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policy on internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. 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, e-bulletins 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 DSLs 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 applicable.

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

12. Monitoring arrangements

The DSLs will log behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed every year by the SLT. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Anti-Bullying Policy
- Behaviour and Discipline Policy
- Child protection and safeguarding policy
- Complaints Policy and Procedure
- Data Protection Policy and privacy notices
- Social Media Policy
- Staff Code of Conduct

These policies can be found on the School Website under – Key Information – Policies.

Appendix 1 – Staff ICT Acceptable Use Policy Agreement

Rainow Primary School
Caring, Learning, Achieving

Staff ICT Acceptable Use Policy Agreement

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 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 will have good access to ICT to enhance their work, to enhance learning opportunities for our young people and will, in return, expect staff 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 the young people 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 (e.g. laptops, email, VLE, iPads, 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 Headteacher, Deputy Head or Computing Subject Leader.

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 only use my personal equipment to record these images if it is password protected.
- I will only use chat and social networking sites in school in accordance with the school's policies.

- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.
- I will only communicate with young people and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- If the data on any device is breached, I will report it to the Headteacher, Data Protection Officer, Deputy Head or Computing Subject Leader.

The school has 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 (iPads/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 programmes.
- I understand the importance of regularly backing up my work.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, 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 GDPR Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that any staff or young person's 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.
- It is my responsibility to understand and comply with current copyright legislation.

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 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.

Staff Name:

Signed: **Date:**

Appendix 2a – Rec / KS1 Acceptable Use Policy Agreement

Rainow Primary School
Caring, Learning, Achieving

KS1 Pupil Acceptable Use Policy Agreement

Our aim:

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- Always keep my passwords a secret.
- Only open pages which my teacher has said are OK.
- Only work with people I know in real life.
- Tell my teacher if anything makes me feel scared or uncomfortable on the internet.
- Make sure all messages I send are polite.
- Show my teacher if I get a unkind message.
- Not reply to any unkind messages or anything which makes me feel uncomfortable.
- Only email / message people I know or if my teacher agrees.
- Only use emails / messaging which the school allow.
- Talk to my teacher before using anything on the internet.
- Not tell people about myself online (I will not tell them my name, anything about my home, family and pets)
- Not upload photographs of myself without asking a teacher.
- Never agree to meet a stranger.
- Look after and respect the school ICT equipment.

I know that:

➢ Anything I do on the computer may be seen by someone else.

➢ The CEOP report button is there to keep me safe online and I know when to use it.

Appendix 2b - KS2 Acceptable Use Policy Agreement

Rainow Primary School
Caring, Learning, Achieving

KS2 Pupil Acceptable Use Policy Agreement

Our aim:

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- Always keep my passwords a secret.
- Only use, move and share personal data securely.
- Only visit sites which are appropriate.
- Work in collaboration only with people my school has approved and will deny access to others.
- Respect the school network security.
- Make sure all messages I send are respectful.
- Show a responsible adult any content that makes me feel unsafe or uncomfortable.
- Not reply to any nasty message or anything which makes me feel uncomfortable.
- Not use my own mobile device in school unless I am given permission.
- Only give my mobile phone number to friends I know in real life and trust.
- Only email / message people I know or approved by my school.
- Only use email messaging which has been approved by the school.
- Discuss and agree on my use of a social networking site with a responsible adult before joining.
- Always follow the terms and conditions when using a site.
- Always keep my personal details private. (my name, family information, the journey to school, my pets and hobbies are all examples of personal details)
- Always check with a responsible adult before I share images of myself or others.
- Only create and share content that is legal.
- Never meet an online friend without taking a responsible adult that I know with me.

I know that:

➢ The CEOP report button is there to keep me safe online, and I know when to use it.

➢ Anything I share online may be monitored.

➢ Once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Appendix 3 –Parent / Carer ICT Acceptable Use Policy Agreement

Rainow Primary School
Caring, Learning, Achieving

Parent/Carer - ICT Acceptable Use Policy Agreement

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. 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 ICT 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 eSafety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement can be found as an appendix of the School e-safety policy.

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.

Parent Permission Form

Parent/Carer's Name:

Pupil Name:

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

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – 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 e-safety.

Signed: **Date:**