



# Online Safety Policy

*keeping us safe in  
the digital world*

Policy owner	<b>Senior Leadership Team</b>
Author	<b>Chris Harris, Deputy Principal</b>

## Approved by

Consultation Group	<b>Senior Leadership Team (SLT)</b>
Approval Committee	<b>Academy Council</b>
Implementation Date	<b>April 2025</b>
Review Date	<b>April 2026</b>

## Version Control

<b>Version</b>	<b>Summary of Changes</b>	<b>Consultation Group</b>	<b>Effective Date</b>
2.0	A significant update to policy:  Expanded roles and responsibilities for	SLT	April 2025

	<p>governors, DSL team, and Staff.</p> <p>Updated procedures for educating parents about online safety and the removal of the standard letter.</p> <p>Expanded cyberbullying section, which broadens the section on Examining Electronic Devices and provides a new section on the use of Artificial Intelligence (AI).</p> <p>General update to the use of DSL team rather than named individuals.</p>		
--	---	--	--

# Contents

<b>1. Aims .....</b>	<b>4</b>
1.2 The four key categories of risk.....	4
<b>2. Legislation and guidance .....</b>	<b>4</b>
<b>3. Roles and responsibilities .....</b>	<b>5</b>
3.1 The Academy Council.....	5
3.2 The Executive Principal.....	6
3.3 The Designated Safeguarding Lead (DSL) Team.....	6
3.4 IT support (TIO) .....	7
3.5 All staff and volunteers .....	8
3.6 Parents .....	8
3.7 Visitors and members of the community.....	9
<b>4. Educating pupils about online safety .....</b>	<b>9</b>
<b>5. Educating parents about online safety.....</b>	<b>10</b>
<b>6. Cyberbullying .....</b>	<b>11</b>
6.1 Definition.....	11
6.2 Preventing and Addressing Cyberbullying .....	11
6.3 Examining Electronic Devices .....	12
6.4 Artificial intelligence (AI) .....	13
<b>7. Acceptable use of the Internet in school.....</b>	<b>14</b>
<b>8. Pupils using mobile devices in school .....</b>	<b>14</b>
<b>9. Staff using work devices outside of school .....</b>	<b>15</b>
<b>10. How the school will respond to issues of misuse .....</b>	<b>16</b>
<b>11. Training .....</b>	<b>16</b>
<b>12. Monitoring arrangements.....</b>	<b>17</b>
<b>13. Links with other policies .....</b>	<b>17</b>
<b>Appendix 1: Raleigh Infant acceptable use agreement (pupils and parents/carers) .....</b>	<b>19</b>
<b>Appendix 2: Admirals acceptable use agreement (pupils and parents/carers) .....</b>	<b>20</b>
<b>Appendix 3: Adult acceptable use agreement (staff, governors, volunteers and visitors).....</b>	<b>21</b>
<b>Appendix 4: Online Safety Training .....</b>	<b>22</b>
<b>Appendix 5: SMART Rules Poster .....</b>	<b>23</b>
<b>Appendix 6: Mobile Device Agreement .....</b>	<b>24</b>

# 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 (including mobile phones)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## 1.2 The four 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, anti-Semitism, 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 scam

## 2. Legislation and guidance

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

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying and cyberbullying: advice for Executive Principals 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 cyberbullying 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 Academy Council**

The academy council has overall responsibility for monitoring this policy and holding the Executive Principal to account for its implementation.

The academy council will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The academy council will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The academy council will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL) team.

The academy council should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The academy council must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the [DfE's filtering and monitoring standards](#), and

discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure 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 interrelated 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 Executive Principal**

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

### **3.3 The Designated Safeguarding Lead (DSL) Team**

Details of the school's DSL team are set out in our safeguarding policy as well as relevant job descriptions.

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

- Supporting the Executive Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the Executive Principal and academy council to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the IT Support (TIO) to make sure the appropriate systems and processes are in place
- Working with the Executive Principal, IT Support (TIO) 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's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring 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 logged and dealt with appropriately in line with the school behaviour policy and anti-bullying policy.
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Executive Principal and/or academy council
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

### **3.4 IT support (TIO)**

IT support is provided by Turn It On (TIO) and 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 a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL team is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by alerting the DSL team for an immediate response
- Following the correct procedures by getting authorisation from the Executive Principal and then contacting IT Support (TIO) if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the safeguarding team 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 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 Parents**

Parents are expected to:

- Notify a member of staff or the Executive principal of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 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](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)

### **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. Educating pupils about online safety**

Pupils will be taught about online safety as part of the curriculum using the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

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
- Use the SMART on-line safety rules (Stay **S**afe, don't **M**eeet up, don't **A**cccept files or requests, how **R**eliable is the information, **T**ell an adult) [www.kidsmart.org.uk](http://www.kidsmart.org.uk) (See Appendix 5)

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
- Use the SMART on-line safety rules (Stay **S**afe, don't **M**eeet up, don't **A**cccept files or requests, how **R**eliable is the information, **T**ell an adult) [www.kidsmart.org.uk](http://www.kidsmart.org.uk) (See Appendix 5)

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

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.

## **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. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

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

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

If a child shares that they have watched or accessed age-inappropriate technology, video, television, social media, etc., their parent/carer will be contacted to discuss ways to keep their child safe.

## **6. Cyberbullying**

### **6.1 Definition**

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is persistently, deliberately hurtful or threatening and targeted behaviour. It is not a one-off isolated incident. See also the school behaviour policy and anti-bullying policy.

### **6.2 Preventing and Addressing Cyberbullying**

To help prevent cyberbullying, 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 witnesses rather than victims.

The school will actively discuss cyberbullying 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 cyberbullying, its impact and ways to support pupils as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyberbullying 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 cyberbullying, the school will follow the processes set out in the school behaviour 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 DSL team will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

All online safety concerns are recorded on CPOMS and are regularly reviewed by the DSL team.

### **6.3 Examining Electronic Devices**

The Executive Principal and any member of staff authorised to do so by the Executive Principal 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 the Executive Principal
- 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 co-operation

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 Executive Principal 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/carer 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 team immediately, who will decide what to do next. The DSL team 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.

## **6.4 Artificial intelligence (AI)**

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils very seriously, in line with our behaviour and anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where the school is using new AI tools and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

## **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 1-3). 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, 2 and 3.

## **8. Pupils using mobile devices in school**

Mobile devices include, but are not limited to, mobile phones, smart watches or any other digital device capable of recording and/or sending text, sound, images, data or video.

If a pupil has a mobile device agreement (appendix 6) signed by a parent/carer then they may bring mobile devices into school. Mobile devices must be switched off before coming on site.

At the start of the day, all pupils must turn off their mobile devices before coming on site. They must place their devices into a named bag and hand them to the adult in charge of their class. The mobile device will be stored in a lockable box and placed in a cupboard in the classroom. The mobile device will be returned to the pupils at the end of the school day.

If a child has a mobile device switched on whilst on site then this will be a breach of the mobile device agreement and could lead to the pupil being banned from having a mobile device on site.

Exceptions to the mobile device agreement, e.g. for medical reasons – such as blood sugar tracking, must be authorised in writing by the Executive Principal as part of a health care plan.

## **9. 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)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

IT support will also help by:

- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

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 3.

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 IT support.

## **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 policies on behaviour and ICT and 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 disciplinary procedures. 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 the risks up
- 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 Team 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**

CPOMS is used to log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL Team. At every review, the policy will be shared with the academy council. 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:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

## Appendix 1: Raleigh Infant acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it
- I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:

## Appendix 2: Admirals acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or safe adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

Signed (pupil):

Date:

**Parent/carer's agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

## Appendix 3: Adult acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and IT support know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

## Appendix 4: Online Safety Training

Online safety training needs – Self-Audit	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
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?	

# Appendix 5: SMART Rules Poster



The poster features a red background with a green sticky note at the top left containing the title 'Be smart on the internet'. To the right of the sticky note are illustrations of a laptop, a mobile phone, and a mouse. In the top right corner is the Childnet International logo and website address. The main content is organized into five horizontal bars, each representing a rule: 'S SAFE' (yellow bar), 'M MEETING' (green bar), 'A ACCEPTING' (blue bar), 'R RELIABLE' (green bar), and 'T TELL' (yellow bar). Each rule includes a brief explanation and a small icon. At the bottom, there is a blue bar with the website 'www.kidsmart.org.uk', a KidSMART logo, and a cartoon character. A vertical copyright notice is on the far right edge.

**Be smart on the internet**

Childnet International  
www.childnet.com

**S SAFE** Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.  ZIP IT

**M MEETING** Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time. 

**A ACCEPTING** Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!  BLOCK IT

**R RELIABLE** Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows. 

**T TELL** Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.  THINK U KNOW  
You can report online abuse to the police at [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)  FLAG IT

**www.kidsmart.org.uk**

**KidSMART** Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world. 

Childnet International © 2010 Registered Charity no. 1000172

## Appendix 6: Mobile Device Agreement

### MOBILE DEVICE agreement for pupils and parents/carers

Name of pupil:

Mobile devices include, but are not limited to, mobile phones, smart watches or any other digital device capable of recording and/or sending text, sound, images, data or video.

I agree to do the following:

- I will turn off all mobile devices before coming on to the academy site.
- As soon as I am in class, I will place all my mobile devices into my named bag.
- I will hand my named bag to the adult in charge of my class.

My mobile devices will be stored in a lockable box and placed in a cupboard in the classroom.

At the end of the school day, my mobile devices will be returned to me.

I will not turn on my mobile devices until I am off site.

I agree that the academy may check, at any time, that my mobile devices are switched off.

I understand that if I don't follow this agreement then my mobile devices may be confiscated and held at the office for a parent/carer to collect.

I understand that, for any reason, the academy may withdraw permission for me to bring my mobile devices to school.

Signed (pupil):

Date:

Parent/carer agreement:

I agree that my child may bring mobile devices to school.

I agree that the academy does not accept any responsibility for loss or damage to any mobile device.

I understand that should my child not follow the mobile device agreement, then the mobile device may be confiscated and held at the school office for a parent/carer to collect.

The academy may withdraw permission for my child to bring mobile devices to school for any reason.

Signed (parent/carer):

Date: