Online Safety Policy

O you who believe, uphold justice and bear witness to Allah, even if it is against yourselves, your parents, or your close relatives. Whether the person is rich or poor, Allah can best take care of both. Refrain from following your own desire, so that you can act justly- if you distort or neglect justice, Allah is fully aware of what you do.
Quran 4:135

Approved by:	Governing Board	**Last reviewed:** Summer 2025
Next review due by:	Summer 2026	

1. Aims

Our Online Safety Policy has been written to protect pupils, staff and governors by providing clear advice and guidance. We aim to implement robust and inclusive processes that safeguard all members of the school community—through education, clear response mechanisms, and responsible use of technology.

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
- **Contact** – being subjected to harmful online interaction with other users
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm
- **Commerce** – risks such as online gambling, inappropriate advertising, 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
- [Relationships and sex education
- Searching, screening and confiscation
- DfE's guidance on protecting children from radicalisation.

3. Roles and responsibilities

3.1 Leadership team and governors	3.2 The designated safeguarding lead (DSL)	3.3 ICT Manager
Online Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of governors, aims to embed safe practices into the culture of the school. The leadership along with the DSL ensures that the policy is implemented and compliance with the policy is monitored. The governor who oversees online safety is the *safeguarding link governor*.	The DSL takes lead responsibility for online safety in school, in particular: o Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks o Working with the ICT manager to make sure the appropriate systems and processes are in place o Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents o Ensuring that any online safety incidents are logged o Ensuring that any incidents of cyber-bullying are logged on Behaviour log or Cura as appropriate	The ICT manager is responsible for: o Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks o Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

3.4 Staff and volunteers	3.5 Pupils
All staff, including contractors and agency staff, and volunteers are responsible for: o Maintaining an understanding of this policy o Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use (see appendices) o Knowing that the DSL 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 informing the DSL Working with the DSL to ensure that any online safety incidents are logged On Cura and dealt with appropriately in line with this policy	Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with online safety issues, both at home and school **3.6 Parents/carers** Parents/carers are expected to notify a member of staff or the headteacher of any concerns or queries regarding this policy and support these rules with their children. The school will raise parents' /carers' awareness of internet safety in letters or other communications home, and in information via our website. It also will be covered in Safeguarding sessions for parents. Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites: o What are the issues? – UK Safer Internet Centre o Hot topics – Childnet o Parent resource sheet – Childnet

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

5. Cyber-bullying

5.1 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 school behaviour policy.)*

5.2 Preventing and addressing 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
- 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.

5.3 Artificial intelligence (AI)

Noor ul Islam Primary School recognises 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. The school will treat any use of AI to bully pupils in line with our Behaviour and Anti-Bullying policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed.

6. Acceptable use of the internet in school

6.1 All pupils, parents/carers, 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.

6.2 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.

6.3 We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

7. Staff using work devices outside school

7.1 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

7.2 Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

7.3 Work devices must be used solely for work activities.

7.4 If staff have any concerns over the security of their device, they must seek advice from a member of the DSL team.

8. How the school will respond to issues of misuse

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

8.2 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.

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

9. Training

9.1 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.

9.2 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).

10. 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
- Complaints Policy
- Acceptable Internet Use Policy (see appendix)

Appendix 1

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff and other adults				Pupils and young people			
Communication Technologies	**Permitted**	**Permitted at certain times**	**Permitted for specific staff**	**Not Permit-ted**	**Permitted**	**Permitted at certain times**	**Allowed with staff permission**	**Not Permit-ted**
Mobile phones may be brought to school	✓							✓
Mobile phones used in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photographs on mobile devices				✓				✓
Use of PDAs and other educational mobile devices	✓				✓			
Use of school email for personal emails				✓				✓
Social use of chat rooms/facilities				✓				✓
Use of social network sites			✓				✓	
Use of educational blogs	✓				✓			

Appendix 2

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business				✓	

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by our ISP and / or the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non- educational)				✓	
On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Downloading video broadcasting e.g. Youtube	✓				
Uploading to video broadcast e.g. Youtube			✓		

Appendix 3

Incident involving pupils	**Teacher to use school behaviour policy to deal with**	**Refer to Headteacher**	**Refer to police**	**Refer to technical support staff for action re security/filtering**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device.	✓			
Unauthorised use of social networking/ instant messaging/ personal email	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another pupil's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		✓

Continued infringements of the above, following previous warnings or sanctions		✓	Community Police Officer referral	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

Appendix 4

Incidents involving members of staff	**Refer to the Headteacher** ***See below**	**Refer to technical support staff for action re filtering, security etc**	**Referral to WF LADO** **Potential Disciplinary Action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out	✓	✓	✓

digital communications with pupils/ pupils			
Actions which could compromise the staff member's professional standing	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓		✓

***In event of breaches of policy by the Headteacher, refer to the Chair of Governors**

Appendix 5

EYFS & Key Stage 1: Acceptable Internet Use Policy

This is how I keep **SAFE online**:

1. I only **USE** ICT systems like computers or games on websites if a trusted adult tells me I can use one
2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. I will be kind to others and not upset or be rude to them online and I know anything I do online can be shared and might stay online **FOREVER**
8. I don't keep ~~**SECRETS**~~ or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I don't change **CLOTHES** or get undressed in front of a camera
10. I always check before **SHARING** personal information (my name, address or telephone numbers)
11. I only use the username and password I have been given and never share my password with anyone, including my friends
12. I will look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly

My trusted adults are at school and at home.

Appendix 6

Key Stage 2: Acceptable Internet Use Policy

1. I **use** the internet for learning and fun – at school or at home, I follow the same rules.
2. I behave online like I do in class – **kind, safe, respectful.**
3. I **only** use apps, sites, and games I'm allowed to.
4. I **ask** before I download or click on things.
5. I keep my **passwords** private. Friends don't share passwords.
6. I talk and play with people I know in **real life** or who an adult says are okay.
7. I know not everyone **online** is who they say they are.
8. I don't do **live** videos or video chats without checking with an adult.
9. I keep my body **private** on camera and in photos or videos.
10. I say **no** to dares, secrets, or anything that feels wrong.
11. If I see or hear something bad, I don't share it – I **tell** an adult.
12. If I feel **worried**, upset or unsure, I talk to a trusted adult.
13. I follow **age** rules – I don't use 13+ or 18+ games or apps.
14. I keep personal information **private**, like my name, address or school.
15. I **think** before I share – things online can last forever.
16. I treat others kindly and never bully or **exclude** them online.
17. I **report** bad behaviour and block bullies.
18. I **respect** people's work and use safe search tools to check facts.

I understand these rules and will ask for help if I need it.

Appendix 7

Acceptable Internet Use Policy – Staff, Volunteers, Governors and Contractors

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 are powerful tools, which open up new opportunities for everyone. These technologies can inspire 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 always have an entitlement to safe Internet access.

This policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- All Noor Ul Islam ICT systems users are protected from accidental or deliberate misuse that could put the security of the systems or 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 and volunteers will have good access to ICT to enhance their work, to improve learning opportunities for all and will, in return, expect staff and volunteers to agree to be responsible users.

Responsible Use Agreement

I understand that I must use Noor Ul Islam 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 learners 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 pupils.

For my professional and personal safety:

- I understand that the school will monitor my use of ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the school ICT systems (e.g. laptops, email, Learning Platform etc.) out of the school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username and 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/incident I become aware of to the appropriate person (see policy flowcharts).

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.

- I will not use chat and social networking sites in the school in accordance with the school's policies.
- I will only communicate with pupil 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.

Noor Ul Islam Primary School have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal handheld/external devices (PDAs/laptops/mobile phones/USB devices etc) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school's equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any 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 ensure that my data is regularly backed up, in accordance with relevant policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not (unless I have permission) 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 understand that data protection policy requires that any staff or learner 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 policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of Noor Ul Islam Primary School ICT equipment in school, but also applies to my use of school ICT systems and equipment out of the school and my use of personal equipment in the school or in situations related to my employment by Noor Ul Islam Primary 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.