E-Safety Policy

1. Introduction and Aims

1.1. The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet.

1.2. New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

1.3. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

1.4. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

1.4.1. Access to illegal, harmful or inappropriate images or other content including the promotion of extremist groups or ideologies
1.4.2. Unauthorised access to, loss of or sharing of personal information.
1.4.3. The risk of being subject to grooming by those with whom they make contact on the Internet.
1.4.4. The sharing/distribution of personal images without an individual's consent or knowledge.
1.4.5. Inappropriate communication/contact with others, including strangers.
1.4.6. Cyber-bullying.
1.4.7. Access to unsuitable video/Internet games.
1.4.8. An inability to evaluate the quality, accuracy and relevance of information on the Internet.
1.4.9. Plagiarism and copyright infringement.
1.4.10. Illegal downloading of music or video files.
1.4.11. The potential for excessive use which may impact on the social and emotional development and learning of the young person.

1.5. Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically, Anti-Bullying, Behaviour, and Safeguarding.

1.6. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

1.7. The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

2. Scope

2.1. This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteacher, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

2.2. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

3. Roles & Responsibilities

3.1. This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

3.2. Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body (Amin Laher), has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

3.2.1. Meetings with the E-Safety Coordinator
3.2.2. Regular monitoring of e-safety incident logs
3.2.3. Monitoring of filtering/change control logs
3.2.4. Reporting to relevant Governors and/or committee(s) meetings.

3.3. Headteacher & Senior Leadership Team (SLT)

The Headteacher is responsible for ensuring:

3.3.1. The safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety may be delegated to the ***E-Safety co-ordinator.***
3.3.2. Adequate training is provided
3.3.3. Effective monitoring systems are set up
3.3.4. That relevant procedure in the event of an e-safety allegation are known and understood.
3.3.5. Establishing and reviewing the school e-safety policies and documents (in conjunction with e-safety co-ordinator)
3.3.6. The school's Designated Safeguarding Leads should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

3.4. E-Safety Coordinator

The E-Safety Coordinator takes day to day responsibility for e-safety issues and has a leading role in:

3.4.1. Liaising with staff, ICT Technical staff, E-Safety Governor and the Headteacher on all issues related to e-safety;
3.4.2. Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
3.4.3. Providing training and advice for staff;
3.4.4. Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
3.4.5. Co-ordinating and reviewing e-safety education programme in school

3.5. **Teaching & Support Staff**

In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

3.5.1. They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
3.5.2. They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
3.5.3. E-safety issues are embedded in all aspects of the curriculum and other school activities
3.5.4. Students understand and follow the school's e-safety and acceptable usage policies
3.5.5. Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
3.5.6. They monitor ICT activity in lessons, extracurricular and extended school activities
3.5.7. In lessons, internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

3.6. **Students (to an age appropriate level)**

3.6.1. Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
3.6.2. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
3.6.3. Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

3.7. **Parents/Carers**

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

3.7.1. Endorsing (by signature) the Pupil Acceptable Usage Policy.
3.7.2. Accessing the school website in accordance with the relevant school Acceptable Usage Policy.
3.7.3. Reading, understanding and signing the E-Safety Disclaimer

3.8. **Community Users**

Community Users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to sign a Volunteer User AUP (see Appendix 6) before being provided with access to school systems.

4. **Education and Training**

4.1. E-safety education will be provided in the following ways:
  4.1.1. A planned e-safety programme is provided as part of the form tutor and assembly programme and is regularly revisited in PSHE and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
  4.1.2. Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
  4.1.3. Students are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
  4.1.4. Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
  4.1.5. Rules for the use of ICT systems and the Internet are posted in school
  4.1.6. Staff act as good role models in their use of ICT, the Internet and mobile devices.

5. **Acceptable Usage Policy (see Appendix 5/6)**

5.1. **Parents/carers** will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules
5.2. **Staff and regular visitors** to the school have an AUP that they must read through and sign to indicate understanding of the rules.

6. **Copyright**

6.1. Students to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
6.2. Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
6.3. If using a search engine for images – staff / children should open the selected image and go to it's website to check for copyright.

7. **Staff Training**

7.1. E-safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
7.2. All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Safeguarding Policies.
7.3. The E-Safety Coordinator/SLT link will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
7.4. Governors are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or safeguarding.

8. **Communication**

8.1. **Email**

  8.1.1. Digital communications with pupils (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems (see staff guidance in Safeguarding policy as well as the Staff Code of Conduct).
  8.1.2. The school's e-mail service should be accessed via Outlook at school by opening Outlook once logged onto the PC in your own log-on area. Alternatively, it can be accessed via the web-based interface from mail.noorulislam.org.uk

8.1.3. Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.

8.1.4. School e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ pupils.

8.2. **Mobile Phones**

8.2.1. Staff should not be using personal mobile phones in school during working hours when in contact with children.

8.3. **Social Networking Sites**

8.3.1. Young people will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

8.3.2. Staff should not access social networking sites on school equipment in school or at home. Staff should access sites using personal equipment.

8.3.3. Staff users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog**.**

8.3.4. Students/Parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.

8.3.5. If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.

8.3.6. Students in the KS2 curriculum will be taught about e-safety on social networking sites as we recognise some may use it outside of school.

8.4. **Digital Images**

8.4.1. The school record of parental permissions granted/not granted must be adhered to when taking images of our students. Staff can refer to the office for the most up to date details and a copy is provided at the back of the class registers.

8.4.2. Under no circumstances should images be taken using privately owned equipment.

8.5. Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information.

8.6. **Removable Data Storage Devices**

8.6.1. Only school provided removable media should be used

8.6.2. All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks.

8.6.3. Students should not bring their own removable data storage devices into school unless asked to do so by a member of staff.

8.7. **Web sites**

8.7.1. In lessons Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

8.7.2. Staff will preview any recommended sites before use.

8.7.3. "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information.

8.7.4. If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents** will be advised to supervise any further research.

8.7.5. **All** users must observe copyright of materials published on the Internet.

8.7.6. Teachers will use professional judgement regarding which students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the students on the internet by the member of staff setting the task and not them being allowed to as they please. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed. Students are also aware that all internet use at school is tracked and logged.

8.7.7. The school only allows the E-Safety Co-ordinator, ICT technical support and SLT to access to Internet logs.

9. Website filtering

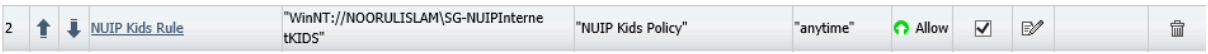
9.1.1. All students log on to Microsoft Active Directory

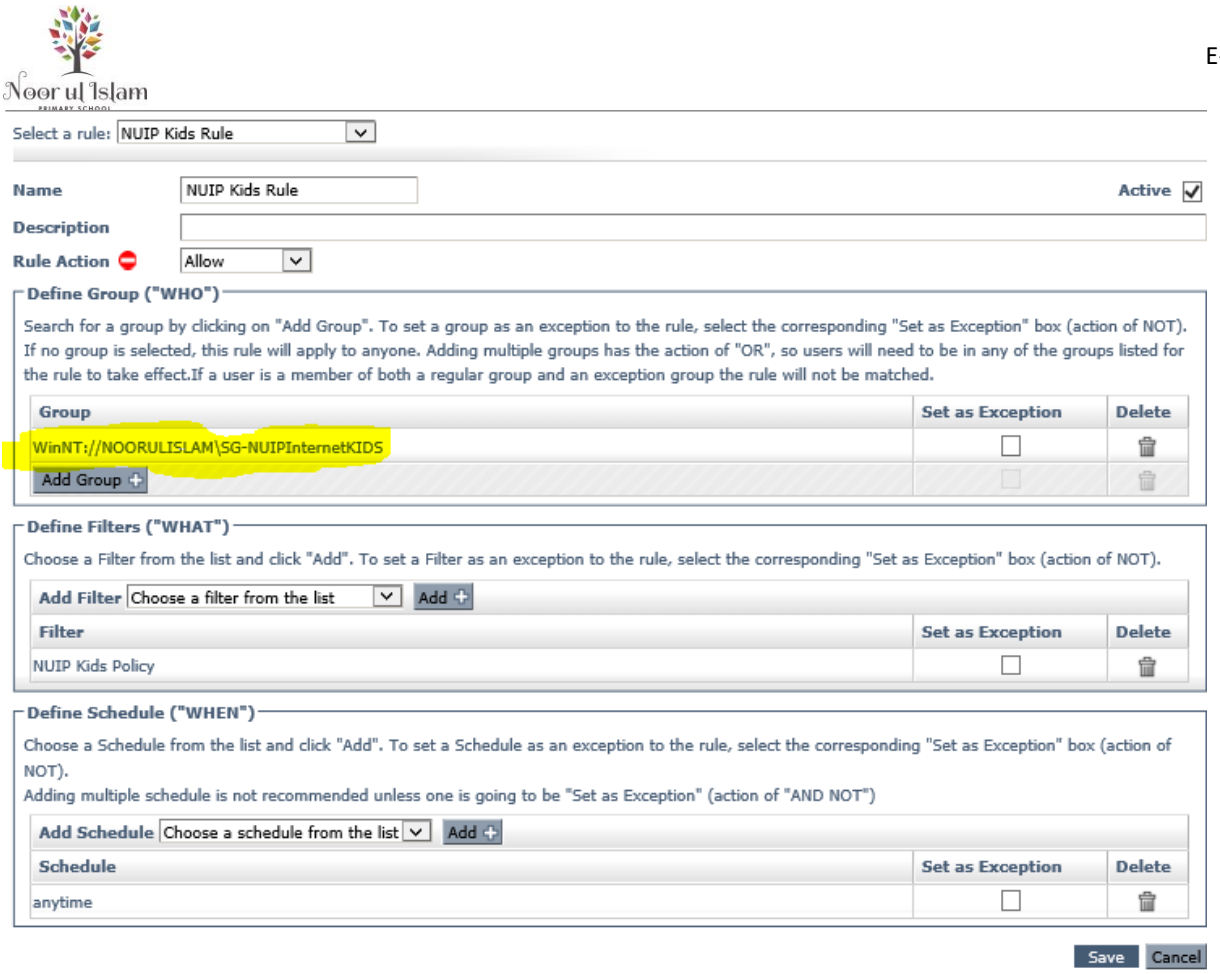
9.1.2. The students account has been added to certain security groups which restricts what they can do on the devices they are logging on to i.e.:

- 9.1.2.1. Cannot install software
- 9.1.2.2. Cannot make changes to laptops to circumvent security
- 9.1.2.3. They will only be presented the respective drive in which they need access to their work

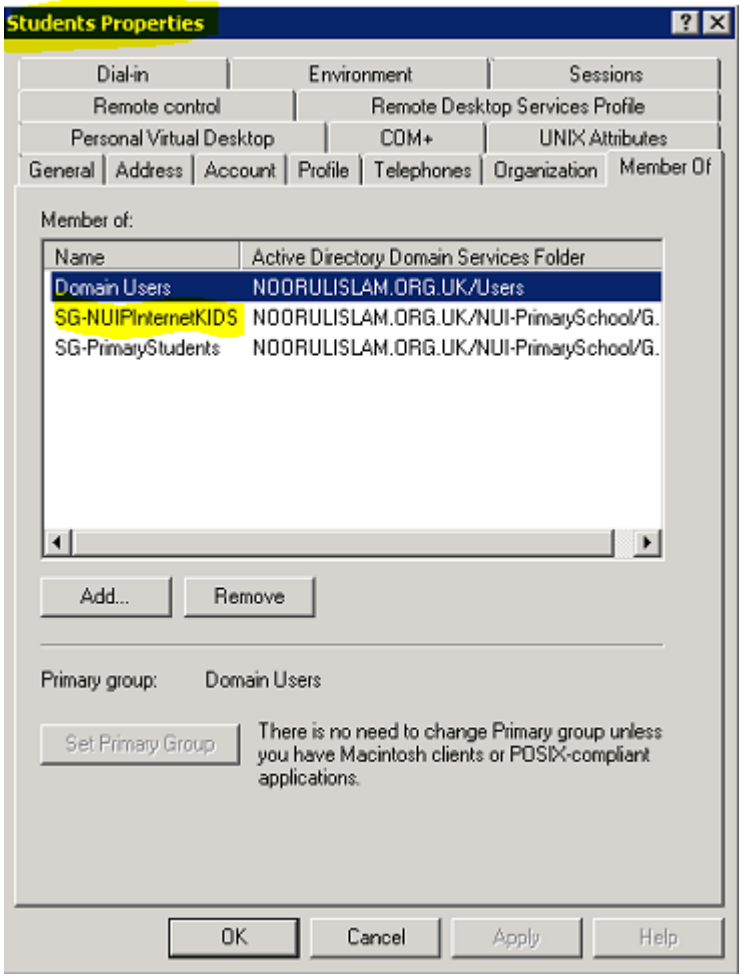
9.1.3. The internet has a web filtering service called Cisco Scansafe and this is a cloud solution.

- 9.1.3.1. This means that:
  - 9.1.3.1.1. All maintenance is done by the providers
  - 9.1.3.1.2. All updates to potential unsafe sites is done by the providers
  - 9.1.3.1.3. All malicious viruses and phishing is updated by the provider
- 9.1.3.2. When students have logged on to our network, all internet traffic is forced through the Cisco Scansafe solution
- 9.1.3.3. All students have a specific internet policy assigned to them so that they cannot visit site which we deem unsafe to them.
- 9.1.3.4. Below are some screen shots of the configuration:





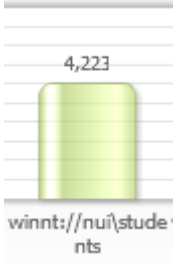
The highlighted demonstrates that if the student account is in the above security group, this policy will be applied to them.



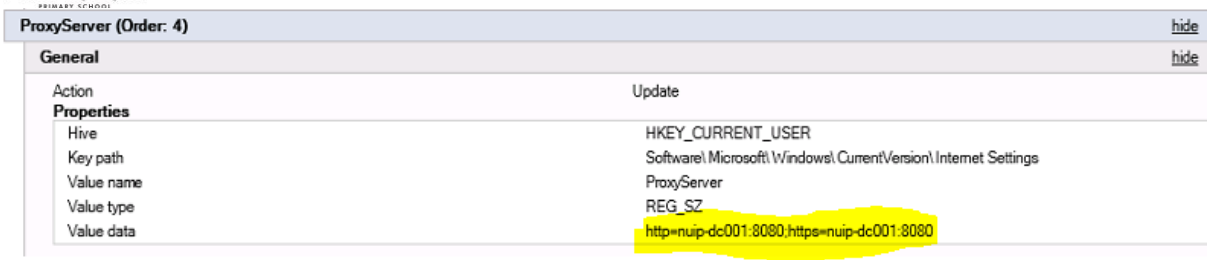
This screen shot demonstrates that the Student account is part of the SG-NUIInternetKIDS security group and will therefore get the policy applied to them.

The above screen shot shows what sites have been **allowed** (or deemed safe) and therefore when a student goes onto a site, if it matches the category then it will be allowed and if it's not ticked then they will be declined from using the site.

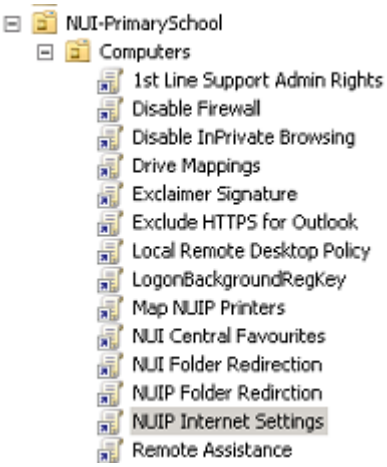
An example of this working is the fact this has been picked up in our dashboard as blocks per user:



Below is a screen shot of how the computers / laptops get the policy applied:



And the policy above is appended to the OU with all Primary school computers:



10. **Passwords**

10.1. **Staff**

10.1.1. Passwords or encryption keys should not be recorded on paper or in an unprotected file
10.1.2. Passwords should be changed at least every 3 months
10.1.3. Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

10.2. **Students**

10.2.1. Should only let school staff know their in-school passwords.
10.2.2. Inform staff immediately if passwords are traced or forgotten. All staff are able to access the network to allow students to change passwords

11. **Use of Own Equipment**

11.1. Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Headteacher.
11.2. Students should not bring in their own equipment unless asked to do so by a member of staff.

12. **Use of School Equipment**

12.1. No personally owned applications or software packages should be installed on to school ICT equipment;
12.2. Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.

12.3. All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

13. **Monitoring**

13.1. All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school's external provider. Whenever any inappropriate use is detected it will be followed up by the E-Safety Co-ordinator or Headteacher depending on the severity of the incident.

13.2. The E-Safety Coordinator and ICT Consultant will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems, the logs will be analysed on a half termly basis.

13.3. Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the e-safety co-ordinator and impounds the equipment and or isolates the equipment being used by others. This is part of the school safeguarding protocol. (If the concern involves the E-Safety co-ordinator then the member of staff should report the issue to the Headteacher).

14. **Incident Reporting**

14.1. Any e-safety incidents must immediately be reported to the Headteacher (if a member of staff) or the E-Safety Coordinator (if a student) who will investigate further following e-safety and safeguarding policies and guidance.

15. **Responding to incidents of misuse**

15.1. It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted.

15.2. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

15.3. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows (Appendix 3 for students and Appendix 4 for staff respectively).

Appendix 1

Communications

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				Students and young people			
Communication Technologies	Permitted	Permitted at certain times	Permitted for specific staff	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
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		✓				✓			

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (in accordance with the school policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

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				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by our ISP and / or the school				✓	

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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 students	**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 etc**
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 student'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		✓		✓

The guidance in this policy should be implemented with cross reference to the School's Child Protection, Anti-Bullying and Behaviour Policies. Note, attempts have been made to synchronise guidance and sanctions.

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 students/ 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

Acceptable Internet Use Policy – Students

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal hand held devices (e.g. mobile phone/ipod) in school at times that are permitted. This commuting to and from school, or to contact parents after participation in an extra- curricular activity. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Signed ……..

Date ……

Appendix 6

Acceptable Internet Use Policy – Staff and Volunteers

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 have an entitlement to safe Internet access at all times.

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 students.

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 student 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 hand held/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.

I have read and understand the above and agree to use the Noor Ul Islam Primary School (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/Volunteer

Name ……..

Signed …….

Date ……..