Nishkam School Trust

Online Safety Policy

Approved by	Trustees	Date: 1 June 2020
Last date of review	22 May 2020	

Contents

Our Vision and Ethos

Nishkam schools are Sikh ethos multi faith schools that take a distinctive approach to many traditional faith schools. The Nishkam School Trust education model is led by virtues such as, compassion, humility, service, contentment, optimism, trust and forgiveness. Virtues are prevalent throughout our teaching and learning model and are modelled by our pupils, staff and teachers. Our pupils explore the divine context of humanity and wonder of all creation and also learn from the wisdom of all religions and in doing so explore the infinite human potential to do good unconditionally. We support all pupils and staff to develop aspects of their own religious, spiritual or human identities. In service of God, we pray for guidance in this endeavour and forgiveness for the errors we may make.

1. Aims and Scope

NST is committed to the ensuring the online safety and wellbeing of all pupils, staff, volunteers, governors and directors who have access to and are users of NST digital technology systems both in and outside of the school's premises.

We aim to have robust processes in place to establish clear mechanisms to identity, intervene and escalate an incident where appropriate.

The Education and Inspections Act 2006 empowers Principals/ Headteachers 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.

This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the Trust. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 online safety behaviour that take place out of school.

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 cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

The following outlines the online safety roles and responsibilities of individuals within NST.

3.1 The Local Governing Board

The LGB has overall responsibility for monitoring this policy and holding the Principal/Headteacher to account for its implementation. Regular meetings with appropriate staff will be held to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL) as part of the Safeguarding Link Governor role and report their findings to the LGB.

All Governors and Directors will ensure that they have read and understood this policy on annual basis and agree and adhere to the terms of the Trust's Agreement for Acceptable Use of The School's ICT Systems and Internet (Appendix 3).

3.2 The Principal/ Headteacher

The Principal/ Headteacher is responsible for;

- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school;
- That all staff receive the appropriate training and support to carry out their roles and responsibilities related to online safety;
- That there is a system in place to allow for regular monitoring of online safety logs.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and Deputy Designated Safeguarding Lead (DDSL) are set out in the Trust's child protection and safeguarding policy as well relevant job descriptions.

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

- Supporting the Principal/Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the Principal/Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;
- Updating and delivering staff training on online safety;
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the Principal/ Headteacher

This list is not intended to be exhaustive.

3.4 ICT Provider

Those with technical responsibilities are responsible for ensuring:

- Appropriate filtering and monitoring systems are put in place, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;

- That the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Security monitoring on all infrastructure is provided; followed by various automated actions taken on security incidents;
- Access to potentially dangerous sites is blocked and, where possible, prevent the downloading of potentially dangerous files;
- That they keep up to date online safety technical information in accordance with all manufacturers to carry out their online safety role and to inform and update others as relevant;
- That the use of the networks/ internet/ digital technologies is regularly monitored in order that any misuse/ attempted misuse can be reported monthly to the Principal/Headteacher/Trust Lead for Governance and Compliance;
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy and referred to the Principal/ Headteacher;
- Ensuring that any incidents of cyber-bullying are referred to the Principal/ Headteacher.

This list is not intended to be exhaustive.

3.5 All Employees and Staff

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

- Ensuring that they have read and understood this policy on an annual basis and agree and adhere to the terms of **Agreement for Acceptable Use of The School's ICT Systems and Internet** (Appendix 3) and ensuring that pupils follow the **Acceptable Use Agreements of the Trust's ICT systems and the internet for parents/carers and pupils** (Appendix 1 and 2);
- Implementing this policy consistently;
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the NST Behaviour Policy;
- Reporting any suspected misuse or problem to the Principal/Headteacher/ DSL for relevant action/investigation or sanction;
- Ensuring that all digital communications with pupils/parents/colleagues are on a professional level and only carried out using official school systems;
- Ensuring that online safety issues are embedded in all aspects of the curriculum and other activities;
- Ensuring that pupils understand and follow this policy and acceptable use policies;
- Agreeing to only transport, hold, disclose or share personal information about myself or others, as outlined in the school policies. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- Ensure that data protection policy requires that any staff or pupil data to which they have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/trust policy to disclose such information to an appropriate authority.
- Ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Monitor the use of digital technologies, mobile devices, cameras (where allowed);

- Ensure that in lessons where 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.

This list is not intended to be exhaustive.

3.6 Pupils

All pupils will be responsible for;

- Agreeing and adhering to the terms of Acceptable Use Agreement of the Trust's ICT systems and the internet for parents/carers and pupils annually (Appendix 1 and 2);
- Understand the importance of reporting abuse, misuse or access to materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies out of school and that the NST Online Safety Policy 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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, the website, social media and information about national/ local online safety campaigns/ literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on;

- The appropriate use of digital and video images taken at school events; access to parents' sections of the website/ learning platforms; their children's personal devices in the school (where allowed);
- Notify a member of staff or the Principal/Headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on Acceptable Use Agreement of the Trust's ICT systems and internet (appendices 1 and 2)

Parents/carers 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 factsheet - Childnet International

3.8 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 Agreement (Appendix 3).

4. Educating pupils about online safety

The education of pupils in online safety/ digital literacy is an essential part of the school's online safety provision and avoid online safety risks. Online safety should be a focus across the curriculum and staff should reinforce the online safety messages.

- Key online safety messages should be reinforced as part of a planned programmed of assemblies/ tutorial/ pastoral activities;

- Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Primary Phase:

In **Key Stage 1**, pupils will be taught to:

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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Secondary Phase:

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

SMART Rules
Pupils should be aware of the 5 SMART Rules which are published by Childnet International:

S - Safe : Keep safe by being careful not to give out personal information such as your name, email address , home address, school name, phone numbers and photographs.

M - Meeting: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parent's or carers' consent and only when they can be present.

A - Accepting: Accepting emails, instant messages, files or texts from strangers can lead to safeguarding concerns.

R - Reliable: Information you find on the internet may not be true, or someone online may be lying about who they are.

T - Tell: Tell your parent, carer or trusted adult if someone or something makes you feel uncomfortable or worried or if someone you know is being bullied online.

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

Parents and carers play an essential role in the education of their children and the monitoring/regulation of their children's online behaviours. 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.

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

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

Parents receive current information pertaining to on-line safety via the school's social media platforms, letter and texts.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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, computing and other subjects where appropriate.

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

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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

6.3 Examining electronic devices

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

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

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

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

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the **Agreement for Acceptable Use of The School's ICT Systems and Internet** (Appendices 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, employees, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Social Media

NST have a duty of care to provide a safe learning environment for pupils and staff. As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school/\Trust. Employees must adhere to the Data Protection Policies at all times; see the Telecommunications and Computer Use Policy for further guidance.

9. Pupils using mobile devices in school

Primary Phase

- Primary phase pupils are not permitted to bring mobile phones into school.
- Pupils in Year 5 and 6 who travel to school independently can bring a mobile phone into school with parental consent. Phones are handed to the class teacher/school office at the start of the day and are locked away. Phones are then returned at the end of the school day. Pupils are not permitted to have any access or use their phones during the school day and/or in any extended school provision.
- The school is not responsible for the loss, damage or theft of any personal mobile device.

Secondary phase

- Students in Years 7- Year 11 are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes during the school day unless they obtain permission from staff. Phones must be handed in every morning and can be collected when pupils leave school at the end of the school day;
- Sixth Form (Y12 & Y13) students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time;
- The school is not responsible for the loss, damage or theft of any personal mobile device;
- The sending of inappropriate text messages between any school members of the school community is not allowed;
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community;
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

10. Employees using work devices outside school

Employees must adhere to the **Agreement for Acceptable Use of The School's ICT Systems and Internet** (Appendix 3), Safeguarding and Child Protection Policy; Telecommunications and Computer Use Policy and Data Protection Policies at all times a breach could result in disciplinary action;

When working from home or an external location employees must ensure that their device is secure and password protected. They must take all reasonable steps to ensure the security of their work device when using it outside school. **No** USB devices containing data relating to the school must be used on personal laptops/ desktop PC's or work devices

If employees have any concerns over the security of their device, they must seek advice from the ICT provider.

Work devices must be used solely for work activities.

11. 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where an employee misuses the school's ICT systems or the internet, or misuses a personal device under the terms of the Telecommunications and Computer Use Policy and it is considered that this action constitutes misconduct, the matter will be dealt with in accordance with the Employee Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

12. Training

All new employees 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 employees 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).

The DSL and DDSL 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 Safeguarding and Child Protection Policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This policy will be reviewed every two years by the Trust board.

14. Links with other policies

- Safeguarding and Child Protection policy
- Behaviour policy
- Employee Code of Conduct
- Data protection policy and privacy notices
- Telecommunications and Computer Use Policy

15. Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

<table>
<tr><td colspan="2">Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers</td></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">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:
o I click on a website by mistake
o I receive messages from people I don't know
o I find anything that may upset or harm me or my friends
• Use school computers for school work only
• I will 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.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">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 for using personal electronic devices in school, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

16. Appendix 2: KS2, KS3 and KS4 acceptable use agreement

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

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password..
- I will be aware of "stranger danger", when I am communicating on-line.
- 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
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action.

When I use the school's ICT systems (tablets, desktop PC's or laptop's 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
- Always log off or shut down a computer when I'm finished working on it
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

I will not:

- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- 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
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- 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 use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or online video streaming unless my teacher has expressly allowed this as part of a learning activity;
- I will not take or distribute images of anyone without their permission.
- I will immediately report any damage or faults involving equipment or software
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed
- If I bring a personal mobile phone or other personal electronic device into school:
  - I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
  - I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
  - I will not use my own personal devices (USB devices etc.) in school.
  - I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others,

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'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:

17. Appendix 3: Agreement for Acceptable Use of The School's ICT Systems and Internet

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

Name of employees/governor/volunteer:

For my professional and personal safety:

- I understand that the Trust will monitor my use of the school digital technology and communications systems;
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) and to the transfer of personal data (digital or paper based) out of school;
- I understand that the Trust digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down in the NST Telecommunications and Computer Use Policy;
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device 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). 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.
- Use them in any way which could harm the Trust's reputation
- Install any unauthorised software, or connect unauthorised hardware or devices to the Trust's network
- 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;
- Promote private businesses;

I will be professional in my communications and actions when using Trust's 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 and not use aggressive or inappropriate language;
- I will ensure that when I take and/or publish images of others I will only do so with their permission and in accordance with the NST Telecommunications and Computer Use Policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the NST Telecommunications and Computer Use Policy
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my mobile devices in school, in accordance with the NST Telecommunications and Computer Use Policy, in the same way as if I was using school equipment.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policies. Any Trust data/ information will only be stored on my personal OneDrive or SharePoint; paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software to my line manager and the ICT provider however this may have happened.

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 Trust digital technology equipment in school, but also applies to my use of the Trust's systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Trust;
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action and in the event of illegal activities the involvement of the police;
- 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, NST Telecommunications and Computer Use Policy and the Trust's data protection policy.
- I will let the designated safeguarding lead (DSL) and ICT manager 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.

I have read and understand the above and agree to use the digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines

Signed (staff member/governor/volunteer) Date: