North Norfolk Academy Trust

Online Policy

Approved: October 2018
Review: Every 3 years
Next Review: October 2021
Owner: A Richardson
Lead: A Taylor
Date sent to Joint Consultative Committee (if applicable): N/A

Contents

.....

1. Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers, Trustees and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Trust community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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 students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

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

3. Roles and responsibilities

3.1 The Trust board

The Trust board has overall responsibility for monitoring this policy and holding the headteacher/ head of school to account for its implementation.

The Trust board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding leads (DSLs).

The governor/ Trustee who oversees online safety is Gill Pegg.

All governors/ Trustees will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the schools' ICT systems and the internet (appendix 2)

3.2 The headteacher/ head of school

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

3.3 The designated safeguarding lead

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

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

- Supporting the headteacher/ head of school in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher/ head of school, network team and 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 schools' behaviour policies
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher/ head of school and/or governing/ Trust board

This list is not intended to be exhaustive.

3.4 The ICT Team leader

The ICT Team leader is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and for keeping students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the schools' behaviour policies.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of ICT systems and the internet (appendix 2), and ensuring that students follow the terms on acceptable use (appendix 1)
- Working with the DSLs to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher/ head of school of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the ICT systems and internet (appendix 1)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the schools' ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum.

Primary schools

In **Key Stage 1**, students 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

Students 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

Secondary schools

In **Key Stage 3**, students 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

Students in **Key Stage 4** may 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

All schools

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

The school will use assemblies and the support and guidance programme to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The schools will raise parents' awareness of internet safety in letters or other communications home, and in information via websites or virtual learning environments (VLE). This policy will also be shared with parents.

Online safety may also be covered during parents' evenings or other information evenings.

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

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

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 Trust behaviour policy and procedures; the anti- bullying policy (STOP) and the assembly programme.)

6.2 Preventing and addressing cyber-bullying

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

The schools will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and form teachers 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, SMSC days, and other subjects where appropriate.

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

The schools also send and/or make available information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support students who may be affected.

In relation to a specific incident of cyber-bullying, the schools will follow the processes set out in the schools' behaviour policies. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSLs 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 students' 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 students 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 students' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All students, parents, staff, volunteers, Trustees and governors are expected to sign an agreement regarding the acceptable use of the schools' ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the terms on acceptable use if relevant.

Use of the schools' 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 students, staff, volunteers, Trustees, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Students using mobile devices in school

Secondary students may bring mobile devices into school, but are not permitted to use them during:

- Lessons; unless directed to do so by a member of staff for educational purposes.
- Tutor group time
- Clubs before or after school, or any other activities organised by the school.

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1) and the device policy and procedures (appendix 4)

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

Primary students cannot bring mobile devices to school unless there is a specific SEND need and arrangement, or is given express permission at the discretion of the Headteacher/ Head of School.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

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

Work devices must be used solely for work activities and PIN protection must be used on mobile devices.

10. How the school will respond to issues of misuse

Where a student misuses the ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies 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/ Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding policy.

12. Monitoring arrangements

The Student Management Team in conjunction with the DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every 3 years.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Device policy and procedures.

Appendix 1: acceptable use agreement (students and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for students and parents/carers	
Name of student:	
When using the school's ICT systems and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms or access programmes which may have chat-room elements within them • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details • Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision 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 agree that the school will monitor the websites I visit. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly.	
Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, Trustees, volunteers and visitors	
Name of staff member/governor/trustee/volunteer/visitor:	
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 • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and Network/ ICT manager know if a student informs me s/he has 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 students in my care do so too.	
Signed (staff member/governor/trustee/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors, trustees and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4
Devices Policy

How to use your devices appropriately.

Mobile phones and devices and, in particular, the new generation of smart phones, such as the iPhone, now include many functions such as an integrated camera, video recording capability, instant messaging, mobile office applications and mobile access to the internet.

These allow immediate access to email, information on the internet and other functions such as access to social networking sites e.g. Facebook, Twitter and Instagram.

For many young people today the ownership of a mobile phone is considered a necessary and vital part of life. When used creatively and responsibly such devices have great potential to support learning experiences and we in the NNAT believe we should be preparing young people to use such modern technology in a safe and responsible way.

In recent times schools have had incidents where mobile phone use has been a negative feature.

Parents and students should be clear that misuse of mobile phones will not be tolerated.

The following are examples of misuse. The list is not exhaustive. The definition of 'misuse' will be at the discretion of the Headteacher:

- the deliberate engineering of situations where people and/or people's reactions are filmed, recorded or photographed in order to humiliate, embarrass and intimidate by publishing to a wider audience;
- bullying by text, image, sound recording and email messaging;
- the use of a mobile device for 'sexting' (the deliberate taking and sending of provocative images or text messages);
- the posting of material on social network sites with no thought to the risks to one's own reputation or that of others and sometimes with the deliberate intention of causing harm to others;

- making disrespectful comments, misrepresenting events or making defamatory remarks about others;

- the general disruption to learning caused by accessing phones during learning times;

- communication with parents/ carers or outside contacts as a result of in-school events so that the ability of staff to deal with an incident is compromised;

- publishing photographs or information of vulnerable people putting them at additional risk.

Dealing with breaches
Misuse of the mobile device will be dealt with using the same principles set out in the school behaviour policy, with the response being proportionate to the severity of the misuse.

Misuse will lead to the confiscation of the mobile device, communication with parents and the imposition of other sanctions up to and including exclusion from school. It may be reported to the Police.

Students and their parents should be very clear that the school is within its rights to confiscate the device where the guidelines have been breached.

If a device is confiscated, the School will make it clear for how long this will be and the appropriate procedure to be followed for its return;

- at the discretion of the teacher the device will be returned at the end of the lesson
- or the student will be informed that the device can be collected at the end of school day from the Headteacher or nominated senior member of staff.
- the confiscation will be recorded for monitoring purposes.
- the School will ensure that confiscated equipment is stored in such a way that it is returned to the correct person.
- in the case of repeated or serious misuse the device will only be returned to a parent/carer who will be required to visit the school by appointment to collect it.
- where a student persistently breaches the expectations, following a clear warning, or there is a severe breach, the Head may impose an outright ban on bringing a device to school. This may be a fixed period or permanent ban.

Where the device has been used for an unacceptable purpose

- The Headteacher or a designated senior staff member will have the right to view files stored in confiscated equipment and, if necessary, seek the cooperation of parents in deleting any files which are in clear breach of these guidelines unless they are being preserved as evidence.
- Such evidence as is needed will be logged, dated and a record kept of those present when the evidence was found and viewed.

Rules for the Acceptable Use of a mobile device in school by students

Students are allowed to bring mobile devices into school. If they choose to do so it is on the understanding that they agree with the following limitations on its use, namely:

- Devices must be switched off in all classes, corridors and other areas during teaching time. It is not acceptable for them to be put on silent or other modes.

- The device must be kept out of sight during lessons in a bag or jacket pocket.

- No student may take a mobile device into a room or other area where examinations are being held.

- Students can only use devices at break and lunchtimes and not while walking through corridors.

- Devices should only be listened to using earphones. Earphones should not be threaded through clothing.

- The security of the device will remain the student's responsibility at all times.

- If asked to do so, content on the device (e.g. messages, emails, pictures, videos, sound files) will be shown to a senior teacher

Unacceptable use

The school will consider any of the following to be unacceptable use of the mobile phone and a serious breach of the school's behaviour policy resulting in sanctions being taken.

- Photographing or filming staff or other students with or without their knowledge or permission.
- Photographing or filming in toilets, changing rooms and similar areas.
- Bullying, harassing or intimidating staff or students by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites.
- Refusing to switch off a device or refusal to hand over the device at the request of a member of staff.
- Using the device outside school hours to intimidate or upset staff or students will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.
- Using a device outside school hours in such a way that it undermines the values of the school and compromises its ability to fulfil its stated educational aim.

.

Please ensure you are aware of these guidelines and rules. Technology is to be embraced and used for learning and effective communication, but it can never be allowed to be used to make others unhappy or afraid.