North East Learning Trust

E-Safety Policy

Review Date	Reviewer	Approved	Implementation
January 2018	J Barker	January 2018	January 2018
September 2018	J Barker	27 September 2018	1 October 2018
September 2020	J Barker		

INTRODUCTION

The North East Learning Trust as part of the wider safeguarding agenda, is committed to ensuring our school community are prepared to deal with the safety challenges that the use of technology brings. Online Safety depends on effective practice at several levels:

- Responsible ICT use by all staff and students and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband and Wi-Fi access including the effective management of filtering across all devices.

VISION

- To provide a diverse, balanced and relevant approach to the use of technology
- To encourage students to maximise the benefits and opportunities that technology has to offer
- To ensure that students learn in an environment where security measures are balanced appropriately with the need to learn effectively
- To equip students with the skills and knowledge to use technology appropriately and responsibly
- To teach students how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment
- To ensure that all users in the school community understand why there is a need for an Online Safety Policy.

ROLES AND RESPONSIBILITIES

Local Academy Council

The Local Academy Council has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

All members of the Local Academy Council will:

- Ensure that they have read and understand this policy;
- Complete Educare Online Safety Training bi-annually.

The Headteacher

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

The Designated Safeguarding Lead (DSL)

Details of the Academy's DSL and deputy DSL are set out in our child protection and safeguarding policy.

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

- Supporting the Headteacher in ensuring that staff understand the policy and that it is being implemented consistently throughout the Academy;

- Working with the 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;
- Ensuring that all staff have completed the Educare Online Safety Training;
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

The Trust's Head of IT Services

The Head of IT Services is responsible for ensuring:

- appropriate filtering and monitoring systems are in place, and are updated on a regular basis to keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- the Academies ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- a full security check and monitoring of the Academy's ICT systems is conducted monthly;
- that access to potentially dangerous sites is blocked and, where possible, preventing the downloading of potentially dangerous files;
- that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- that any incidents of cyber-bullying are dealt with appropriately in line with the Academy's behaviour policy

This list is not intended to be exhaustive.

All staff

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems, and ensuring that students follow the school's terms on acceptable use
- 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 school behaviour policy
- Completing Educare Online Safety training bi-annually

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the Academy's ICT systems and internet

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

Visitors

Visitors who use the Academy'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.

Educating pupils about online safety

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

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

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

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

The Academies will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents/carers about online safety

The Academies will raise parents/carers awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

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

Cyber-bullying

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 Academy behaviour policy.)

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 Academy will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their tutor groups/class, 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, 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 (see section 11 for more detail).

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.

Students and Parents

Research shows that currently 3% of 5 -7-year olds have a smartphone and 35% age 12 – 15yrs.

Social networking sites such as Facebook and Twitter, as well as instant messaging apps and texts, are an important part of the social lives of young people today. Unfortunately, they can also be used negatively e.g. to bully others. The Trust would like to offer the following guidelines to students and parents to make sure the use of these sites is enjoyable and safe. The majority of use takes place outside of school and so must be managed by parents effectively to avoid problems occurring.

If bullying or other problems occur online, via texts, or other social messaging applications:

As a parent you should:

- Report the bullying to Facebook / Twitter and to the police.
- Keep evidence e.g. the text message or print out from Facebook.
- Block or delete the person who has bullied.
- Change your child's mobile phone number.
- Check the security settings and privacy settings on your child's account. These need to be updated regularly.
- Monitor your child's use of the internet, social networking and gaming sites e.g. review their friends list – do they know who all these people are? You would warn them against talking to strangers on the street, so the same rules apply on line.
- Make sure that your child is careful about who they give their contact details to. In being part of a group, your child might receive unwanted messages, images or videos
- Your child must tell a parent or teacher immediately if they receive an inappropriate image or video (e.g. of a fight taking place) online or through messaging apps. If they just store it on their phone or computer, or even open it and delete it, they could find themselves in trouble with the police at a later date, even if they did not ask for that image to be sent to them - the key message is to tell an adult straight away and not pretend it did not happen.
- Make sure that your child understands that information put online stays there forever. Deleting a message on your computer does not mean that it cannot be recovered by someone else at another time
- Ensure that children under 13 do not have Facebook accounts Please do not involve yourself in the dispute by sending a message yourself as you could then find yourself in trouble as well. Instead report it to Facebook/ Twitter and the police.

Useful information on online safety can be found on:

- Vodafone's digital parenting site
- CEOP's YouTube channel -
- http://www.youtube.com/user/ceop?feature=chclk.
- http://www.vodafone.com/content/index/parents.html

This is full of great resources like advice on parental controls, checking privacy settings with your children, check lists for things to be aware of for different age groups of children and a great digital magazine on all the issues in this area.

- CEOP - www.thinkuknow.co.uk

As a school we will:

- Record all bullying incidents, including cyber bullying as detailed in our anti-bullying policy
- Recommend that you de-activate social media accounts
- Investigate any issues that are brought to our attention. As part of this we may ask students and parents to give evidence of the comments made e.g. print out of Facebook comments or we might ask to read a text. Please do not delete these messages.
- Once an investigation is complete, students proved to be involved in bullying will be sanctioned in line with our behaviour policy e.g. internally excluded or receive an internet ban on the school network.
- Involve the police if necessary

Students should:

- Use social media responsibly e.g. do not make rude, abusive or threatening comments to anyone.
- Only talk to people they know and only accept people they know as friends. They should not give out personal information e.g. address, phone number, e mail address. The same applies to people they may play games against online.
- NEVER go and meet anyone they have met online, Lauren who is 15 could turn out to be Rob who is 45.
- Be careful about who they give your contact details to. In being part of a group, your child might receive unwanted messages, images or videos
- NEVER share passwords
- NEVER download information illegally e.g. music
- Be aware that comments made online or pictures posted are there forever. Deleting a message or image on your computer does not mean that it cannot be recovered by someone else at another time.
- Be aware that friends of friends may be able to see comments, photo's etc because of their privacy settings.
- Check the security settings and privacy settings on their account. These need to be updated regularly.
- MUST tell a parent or a member of staff if they are bullied online, via an instant message app or text.
- MUST tell a parent or another adult immediately if they receive an inappropriate image or video (e.g. of a fight taking place) online or through other messaging apps. If they just store it on their phone or computer, or even open it and delete it, they could find themselves in trouble with the police at a later date, even if they did not ask for that image to be sent to you e.g. you receive through messaging apps.
- Report any bullying to Facebook / Twitter but keep the evidence.
- Block or delete the person who has bullied.

Examining electronic devices

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 Trust's complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in school

Mobile devices are not allowed in school and all Academies within the Trust have in place a Mobile Devices in School Policy.

Any breach by a pupil will trigger disciplinary action in line with the Academy's behaviour policy.

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

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

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

Links with other policies

This online safety policy is linked to the following policies:

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

Contacting students during the school day

In accordance with the Trust's safeguarding procedures, parents/carers should contact students through the main reception / switchboard e.g. if a parent/carer needs to get an urgent message to a student. If a child contacts a parent/carer to say they are feeling ill or upset, the parent/carer should contact the main school reception in order that we can investigate further and then get back to them with more information.

Use of digital media

In our school we are aware of the issues surrounding the use of digital media online, the security of data and images held of children. The Principal is ultimately responsible for the security of any data or images held of children. All members of our school understand these issues and need to follow the school's guidance below.

- Apps/systems which store personal data and digital media will be risk assessed prior to use.
- Personal staff mobile phones or devices will not be used for any apps which record and store children's personal details, attainment or photographs.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.

Publishing student's images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the Web site, particularly in association with photographs, unless specific consent has been granted by parents / carers.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- Work can only be published with the permission of the student and parents.

To comply with the Data Protection Act 1998, we will seek permission from parents/carers before we take photographs or make recordings of pupils. We follow the following rules for any external use of digital images and seek written permission from parents and carers:

- If the pupil is named, we avoid using their photograph.
- If their photograph is used, we avoid naming the pupil.

If showcasing digital video work to an external audience, we take care to ensure that pupils are not referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film. Only images of pupils in suitable dress are used. Examples of how digital photography and video may be used at school include:

- Your child's image being used for presentation purposes around the school; e.g. in class or wider school wall displays or PowerPoint presentations.
- Your child's image being used in a presentation about the school and its work to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Use of social networking and online media

This school asks its whole community to promote this approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse – initial abusive messages should be saved as evidence before blocking the sender.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

School Practice

The school uses social networking sites to share information with students and parents e.g. Academy Facebook site, Art department Facebook site, PE department twitter page, etc. These sites are authorised by the school in advance of use and are therefore closely regulated.