



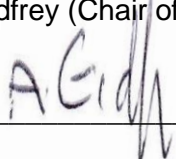
## eSafety Policy

### Policy Version Control

Version history see Annex A errata for details

Version No.	Policy Author	Date Updated	Review Date
1	G Mellefont	01.02 2017	February 2018

**Approval:** A Godfrey (Chair of Board)

 (signed) **Date authorised:** 16.02.2017

This document is the property of North View Academy Trust and its contents are confidential.

*It must not be reproduced, loaned or passed to a 3rd party without the permission of the authoriser. It is controlled within the North View Academy Trust Admin Server where the electronic master is held and can be accessed on a read only basis, subject to security permissions. Users of the document are responsible for ensuring that they are working with the current version.*

*Paper or electronic copies may be taken for remote working etc. However, all paper copies or electronic copies not held within the Admin Server are uncontrolled.*

*Once issued, as a minimum this document shall be reviewed on an annual basis by the originating team/function. To enable continuous improvement, all readers are encouraged to notify the author of errors, omissions and any other form of feedback.*

## **1. What is E-Safety**

Whilst the Internet and associated technologies are an excellent tool and resource to enrich teaching and learning there are still dangers related to their use, especially in relation to young students. Some examples of this are:

- Bullying via chat or email
- Obsessive Internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

As an academy it is our duty of care alongside that of parents and carers to protect our children from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this e-safety policy is to outline what measures the academy takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

## **2. Audience**

This document is intended for parents/carers and academy staff and is a clear outward statement on the academy e-safety practices.

## **3. General policy statement**

The academy will endeavour to ensure e-safety of all academy members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

## **4. Whole academy responsibilities for e-safety**

Within the academy all members of staff and students are responsible for e-safety, responsibilities for each group include:

### Students

- Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions.
- Reporting any e-safety issue to the teacher, learning support assistant or parent.
- Be responsible while using the Internet and any other communication technologies.

### All Staff

- Have a clear understanding of e-safety issues and the required actions from e-safety training sessions.
- Reporting any e-safety issues to the Head Teacher as soon as the issue is detected.
- Compliance with the Acceptable Use Policy which staff must agree to each time the use academy ICT equipment.

### Teaching Staff

- Educating students on e-safety through specific e-safety training sessions and re-enforcing this training in the day to day use of ICT in the classroom.

### ICT Network Manager

- Ensure that the best technological solutions are in place to ensure e-safety as well as possible whilst still enabling students to use the internet effectively in their learning.
- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any e-safety breach.
- Checks and audits all systems to ensure that no inappropriate data is stored or is accessible.

- Works with the Head Teacher and ICT Leader to create, review and advise on e-safety and acceptable use policies.
- Assists in the resolution of e-safety issues with the Head Teacher and other members of staff.
- The Network manager (Mr. Gavin Kershaw) is a trained CEOPs Ambassador.

#### ICT Leader

- Leads the development of the e-safety education programme for students and staff.
- Manages parental awareness for e-safety.
- The ICT Leader (Mr. Colin Bell) is a trained CEOPs Ambassador.

#### Head teacher

- Deals with e-safety breaches from reporting through to resolution in conjunction with the ICT Network Manager.
- Works with the ICT Leader and ICT Network Manager to create, review and advise on e-safety and acceptable use policies.
- Works with outside agencies including the police where appropriate.
- Maintains a log of all e-safety issues.

### **5. How the academy ensures e-safety in the classroom**

#### Educating students in e-safety

A clear objective of the academy is to educate students in safe use of ICT and the Internet. We feel this is one of the best ways to minimise the potential for any e-safety issues to occur.

- Students will receive specific e-safety lessons
- Students know the e-safety risks that exists and how to identify when they are at risk.
- Students know how to mitigate against e-safety risks by using e-safety practices whilst online.
- Students know when, how and whom to report instances when their e-safety may have been compromised.
- Students know that they are in an environment that encourages them to report e-safety issues without risk of reprimand, humiliation or embarrassment.

The academy will follow the Think U Know programme by the governments Childs Exploitation and Online Protection (CEOP) centre as one of the primary education tools.

In addition to this specific training, all members of staff will have a duty to reinforce e-safety practices wherever possible and will offer students advice and support in the classroom where minor e-safety incidents have occurred.

E-safety education information will have high visibility in areas of the academy.

#### **Acceptable Use Policies**

All academy members including students, staff and parents must agree to an Acceptable Use Policy before they can use academy ICT systems. With respect to e-safety the Acceptable Use Policy details:

- The users responsibilities
- Activities which are appropriate and inappropriate
- Best practice guidelines
- How the academy will monitor e-safety

#### **How e-safety is monitored**

- The academy teachers along with the ICT Network Manager will actively monitor the students ICT activity using a monitoring system which will help prevent e-safety issues. (Net Support)
- The ICT Network manager will block any harmful websites that have been reported via teachers that could present an e-safety issue.
- The Head Teacher will periodically review the e-safety log to track any trends and use the information to look at ways of improving the students' e-safety.
- Teaching staff will directly monitor the students ICT and Internet use in the classroom.

#### **How technology is used**

The academy will employ many different technologies to help to ensure-safety for all the academy members:

- The academy will use Internet filtering to block inappropriate content as designated by the Dcfs and Becta and in addition block websites which are irrelevant to the student programme of study and are considered time wasting.
- The academy will use a system which tracks all student activity on the academy computers. The system will aid in flagging up any potential e-safety issues which will be monitored and then can be investigated by the Network Manager and Head Teacher.
- Teaching staff will use close vigilance to monitor all student activity whilst using ICT equipment.

## **6. How the Academy will respond to issues of misuse**

The following are provided for the purpose of example only. Whenever a student or staff member infringes the e-safety policy, the final decision on the level of sanction will be at the discretion of the Head Teacher.

### **Students**

#### **Category A infringements**

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of a mobile phone (or other new technologies)
- Use of unauthorised instant messaging / social networking site

#### **Category B infringements**

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of a mobile phone (or other new technologies) after being warned
- Accidentally accessing offensive material and not notifying a member of staff

#### **Category C infringements**

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

#### **Category D infringements**

- Continued sending of email or instant messages regarded as harassment or of a bullying nature after a warning
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988

### **Staff & Governors:**

#### **Category A infringements (Misconduct)**

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on the ICT network

#### **Category B infringements (Gross Misconduct)**

- Serious misuse of, or deliberate damage to, any school computer hardware or software
- Any deliberate attempt to breach data protection or computer security rules
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the Academy into disrepute

### **Child Pornography:**

In the case of child pornography being found, the member of staff will be immediately suspended and the Academy disciplinary procedures implemented.

### **Other safeguarding actions:**

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop
- Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in school
- Identify the precise details of the material

- Where appropriate, involve external agencies as part of these investigations

### **How will staff and students be informed of these procedures?**

- Procedures are included within the schools e-safety / Acceptable Use Policy. All staff are required to sign the school e-safety policy acceptance form
- Pupils will be instructed about responsible and acceptable use and given strategies to develop “safe behaviours”.
- The academy e-safety policy will be made available to parents who are required to sign an acceptance form when their child starts at school

## **7. Working with parents and the community**

Clearly many academy students will also have access to ICT and the Internet at home, often without some of the safeguards that are present within the academy environment. Therefore parents must often be extra vigilant about their child’s e-safety at home.

One of the goals of the academy is to support parents’ role in providing an e-safe environment for their children to work outside of the academy.

The academy will aid this by:

- Publishing e-safety information and direct parents to external advisories via the academy website.
- Answer any questions that parents may have regarding e-safety

## **8. Acceptable Use Policies**

The academy has the following acceptable use policies in place which must be agreed to before the relevant individuals will be able to access ICT systems and the Internet.

- Staff ICT and the Internet Acceptable Use Policy
- Students ICT and the Internet Acceptable Use Policy
- Academy Internet Access policy

Copies of these policies are available on request; they are also available for download via the academy website. The academy will regularly review and update these policies.

**Annex A**

<b>Version No.</b>	<b>Change History</b>	<b>Guidance reference (if any)</b>	<b>Date</b>
1	Created		01.02.2017