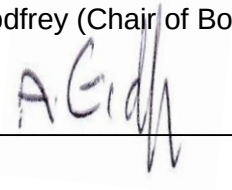
Online Safety Policy

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:** 22.03.2018

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

Audience

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

General policy statement

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

Whole academy responsibilities for online safety

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

Students

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

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 academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the individual academies 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 the parents section of the website and Facebook page

Teaching & Support Staff

- Educating students on online safety through specific online safety training sessions and re-enforcing this training in the day to day use of ICT in the classroom.
- Read, understand and sign the Staff Acceptable Use Policy/Agreement.
- Report any suspected misuse or problem to the Head Teacher.

- All digital communications to parents/pupils/carers must be on a professional level and only carried out using official school systems.
- Ensure pupils understand and follow the online safety and acceptable use policies.
- Monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices.

ICT Network Manager

- Ensure that the best technological solutions are in place to ensure online 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 online safety breach.
- Ensures that users may only access the network and devices through a properly enforced password protection policy.
- Checks and audits all systems to ensure that no inappropriate data is stored or is accessible.
- Works with the Head Teacher and online safety coordinator to create, review and advise on online safety and acceptable use policies.
- Assists in the resolution of online safety issues with the Head Teacher and other members of staff.
- The Network manager (Mr. Gavin Kershaw) is a trained CEOPs Ambassador.
- Ensures the use of the IT system is regularly monitored in order that any misuse/attempted misuse can be reported to the Head Teacher, online safety coordinator for investigation/action/sanction.

Online Safety coordinator

- Leads the development of the online safety education programme for students and staff.
- Manages parental awareness for online safety.
- The online safety coordinator (Mr. Colin Bell) is a trained CEOPs Ambassador.
- Takes day to day responsibility of online safety issues
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- Provide training and advice for staff.
- Receive reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Liaise with Network Manager (Gavin Kershaw)
- Report termly to senior leadership team.

Head teacher

- The Head Teacher has a duty of care for ensuring safety (including online safety) of members of the school community; however the day to day responsibility for online safety will be delegated to the online safety coordinator
- The Head Teacher and other designated safeguarding offices are aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff.
- The Head teacher is responsible for ensuring that the online safety coordinator, Network Manager and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- Deals with online safety breaches from reporting through to resolution in conjunction with the ICT Network Manager.

- Works with the online safety coordinator and ICT Network Manager to create, review and advise on online safety and acceptable use policies.
- Works with outside agencies including the police where appropriate.
- Maintains a log of all online safety issues.
- The senior leadership team will receive termly monitoring reports from the online safety coordinator.

Safeguarding Designated Person

The safeguarding person will be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber bullying
- sexting

How the academy ensures online safety in the classroom

Educating students in online 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 online safety issues to occur.

- Students will receive specific online safety lessons
- Students know the online safety risks that exists and how to identify when they are at risk.
- Students know how to mitigate against online safety risks by using online safety practices whilst online.
- Students know when, how and whom to report instances when their online safety may have been compromised.
- Students know that they are in an environment that encourages them to report online 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 online safety practices wherever possible and will offer students advice and support in the classroom where minor online safety incidents have occurred.

Online 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 online safety the Acceptable Use Policy details:

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

How online 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 online safety issues. (Net Support)
- The ICT Network manager will block any harmful websites that have been reported via teachers that could present an online safety issue.
- The Head Teacher will periodically review the online safety log to track any trends and use the information to look at ways of improving the students' online 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 online safety for all the academy members:

- The academy will use Internet filtering to block inappropriate content 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 online 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.

Unsuitable / Inappropriate Activities

North View Academy believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside of school when using school equipment or systems. This policy restricts usage as follows:

- No mobile phones or cameras will ever be with a member of staff undertaking intimate care tasks.

- Users shall not visit Internet sites, make, post, download, upload, transfer, communicate or pass on, material, remarks, proposals or comments that are classed as illegal or any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Academy or brings it into disrepute.

- Users will not carry out sustained or instantaneous high volume network traffic (downloading / streaming) that causes network congestion and hinders others in their use of the internet.

- Users will not use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.

- Users will not upload, download or transmit commercial software or any copyrighted materials belonging to their parties, without the necessary licensing permissions.

- Users will not reveal or publicise confidential or proprietary information.

- Users will not participate in online gaming that is not for educational purposes.

Managing Email

- All members of staff are provided with a specific academy email address to use for any official communication.
- The use of personal email addresses by staff for any official academy business is not permitted.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Accesses to personal email accounts are not permitted.
- Academy email accounts should not be used for setting up personal accounts e.g. Facebook and Twitter.

Personal Mobile Devices (including phones)

North View Academy has a strict policy regarding the use of personal mobile phones or other electronic communication devices.

Due to the potential of misuse of mobile devices with camera or Internet facilities it is our policy that under no circumstances shall anyone be allowed to bring their mobile phones into any teaching and learning area while pupils are present unless sanctioned by the Head Teacher.

Staff and visitors must ensure that mobile devices are kept in a secure location outside of the teaching and learning areas.

By signing in, staff and visitors have agreed to follow North View Academy's policy on mobile phone use. This must be clearly displayed on entry to each setting.

Under no circumstances does the academy allow staff to contact a pupil or parent/carer using their personal device. The academy is not responsible for the loss, damage or theft of any personal mobile device. The sending of inappropriate messages between any members of the academy community is not allowed. Users bringing personal devices into the academy must ensure there is no inappropriate or illegal content on the device.

Personal Mobile Devices (including phones) – Pupils

Pupils are not allowed to bring personal mobile devices/phones to the academy. Pupils who are found to be disregarding this policy will have their mobile device kept in a secure location within the school office and returned at the end of the day.

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 online safety / Acceptable Use Policy. All staff are required to sign the school online safety policy acceptance form

- Pupils will be instructed about responsible and acceptable use and given strategies to develop “safe behaviours”.
- The academy online safety policy will be made available to parents who are required to sign an acceptance form when their child starts at school

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. An audit of online safety will be carried out on a termly basis.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy’s online safety policy and acceptable use agreements.
- CEOPs training will be provided to all staff by the academy’s CEOPs Ambassador.
- The online safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The online safety coordinator will provide advice / guidance / training to individuals as required.

Training – Trustees / Governors

Trustees / Governors should take part in online safety training / awareness sessions, with particular importance for those involved in technology / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by North View or other relevant organisations.
- Participation in school training / information sessions.

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

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

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.

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 online 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

Annex A

Version No.	Change History	Guidance reference (if any)	Date
1	Created		01.02.2017