Northampton School *for Boys*

E-Safety and Acceptable Use Policy

Approved by:	**Governors' Welfare Committee**
Date:	**13 September 2017**
Review Date:	**September 2018**

Based on policy developed by the Children and Young People's Service in consultation with Education Welfare - CYPS, Northamptonshire Police, the Local Safeguarding Children's Board Northamptonshire, Governors, Parents/Carers and Children, and in partnership with Professional Associates, following Becta Guidelines and review of this policy by Becta.

CONTENTS

What is an AUP (Acceptable Use Policy)?
This Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within the school.

At present the internet technologies used extensively by young people in both home and school environments include:

- Websites
- Social Networking and Chat Rooms
- Gaming
- Music Downloading
- Mobile phones with wireless connectivity
- Email and Instant Messaging
- Learning Platforms
- Video Broadcasting

Despite the significant educational and social benefits associated with the use of these technologies, there are risks which need to be emphasised to all users and steps taken to safeguard against them.

The risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming (usually pretending to be someone younger than their true age).
- Illegal activities of downloading or copying any copyright materials and file-sharing.
- Computer viruses.
- Cyber-bullying.
- "Sexting" the sending of indecent personal images, videos or text via mobile phones.
- On-line content which is biased, abusive or pornographic

2 Roles and responsibilities of the school:

2.1 Governors and Headteacher

It is the responsibility of the Headteacher with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the school.

- The Headteacher is responsible for data and data security in the school. The Headteacher will use approved internet services and that sufficient resource is available to ensure the efficient working of e-safety procedures.

- The Headteacher has designated an e-Safety leader to overview agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment.

- The Headteacher will inform the Governors about the progress of or any updates to the e-Safety curriculum (C&G or ICT) and ensure Governors know how this relates to child protection.

- The Governors will ensure Child Protection is covered with an awareness of e-Safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.

- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures and appropriate action is taken.

2.2 e-Safety Leader
It is the role of the designated e-Safety Leader *along with the Designated Safeguarding Lead to;*

- Monitor the establishment and maintenance of a safe ICT learning environment within the school and report this to the Headteacher.

- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-Safety and for parents to feel informed and know where to seek advice.

- Liaise with ICT support staff to ensure that filtering is set to the correct level for staff, children and young people. Ensure transparent monitoring of the internet and on-line technologies.

- Liaise with the C&G, Child Protection and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technology.

- Update staff training according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.

- Log incidents for analysis to help inform future development and safeguarding, where risks can be identified.

- Work with the Network Manager to ensure the security of the school's network and report any breach or misuse to the Headteacher

- Ensure that internal e-mails fit a professional establishment;
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication

2.3 Adults in school
It is the responsibility of all adults within the school or other setting to:

- Read, understand and sign the Acceptable Use Rules

- Ensure that they know who the Designated Person for Child Protection is within school, so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher and Designated Safeguarding Lead. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.

- Be familiar with the Behaviour policy, Anti-bullying policy, Child Protection policy, Safeguarding policy, personnel and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately.

- Report any concerns about filtering levels to the e-Safety Lead and IT Support.

- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.

- Ensure that students are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.

- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.

- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.

- Report accidental access to inappropriate materials to the e-Safety Leader in order that inappropriate sites are added to the restricted list.

- Report incidents of personally directed "bullying" or other inappropriate behaviour via the internet or other technologies in the same way as for other non-physical assaults.

- Ensure that email is appropriately used – take care when using the school's email account and ensure emails are appropriately worded as such documents can be accessed through the Freedom of Information Act 2000. Staff should not use other email addresses to contact parents or pupils.

2.4 Students

Students will be:

- Required to read, understand and sign the Acceptable Use Rules

- Involved in the review of Acceptable Use Rules through the school council, in line with this policy being reviewed and updated.

- Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new student attends the school for the first time.

- Taught to use the internet in a safe and responsible manner through ICT and C&G.

- Taught to tell an adult about any inappropriate materials, abuse, misuse or contact from someone they do not know straight away.

2.5 Parents

Parents are required to support the school by discussing and agreeing compliance with the Acceptable Use Rules with your child(ren) and speak to the School over any concerns in respect of your child's use of technology

3. Appropriate and Inappropriate Use

3.1 By staff

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access this and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff will receive a copy of the Acceptable Use Policy. The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations.

When accessing the school's systems from home, the same Acceptable Use Rules will apply.

In the event of inappropriate use

If a member of staff is believed to misuse the school's ICT system in an abusive or illegal manner, a report must be made to the Headteacher and Designated Safeguarding Lead immediately and all appropriate authorities contacted. Misuse may result in disciplinary action being taken against the member of staff concerned.

3.2 By Students

Acceptable Use Rules are there for students to understand what is expected of their behaviour and attitude when using the internet which then enables them to take responsibility for their own actions. The School encourages parents/carers to support the rules with their child or young person and this is discussed at their first parents' evening when they start the school.

The rules will be on display within computer rooms around the school.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means on-line should be appropriate and be copyright free when using the schools systems.

The school council are actively involved in discussing the acceptable use of technologies and the rules for misusing them.

In the event of inappropriate use

Should student be found to misuse the on-line facilities whilst at school, one or more of the following consequences may occur;

- Any student found to be misusing the internet by not following the E-Safety and Acceptable Use Rules may have a letter sent home to parents/carers explaining the reason for suspending the student's use for a particular lesson or activity.

- Further misuse of the rules may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.

- A letter may be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

- Sanctions may be imposed for breaching the school's behaviour policy

The normal routes for dealing with problems should be followed with the addition of informing the e-safety leader and/or child protection where appropriate.

In the event that a student **accidentally** accesses inappropriate materials the student should report this to an adult immediately and take appropriate action to hide the screen

Students will be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

4 The curriculum and tools for Learning

4.1 Internet use

Schools and educational settings should teach children and young people how to use the internet safely and responsibly. They should also be taught, through ICT and C&G lessons, how to research information, explore concepts and communicate effectively in order to further learning.

The following concepts, skills and competencies should have been taught by the time they leave *Year 11*:

- Internet literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – know what is safe to upload and not upload personal information
- where to go for advice and how to report abuse

These skills and competencies are taught within the curriculum so that students have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Students should know how to deal with any incidents with confidence.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information.

4.2 E-mail use

Staff and Students should use their school issued email addresses for any communication between home and school only. A breach of this may be considered a misuse and

disciplinary action may be taken under the relevant school policy and procedures against staff and students.

4.3 Mobile phones and other emerging technologies

Such technologies are allowed in school but are the responsibility of the owner. Inappropriate use of such technology would be in breach of this policy e.g:

- images or video taken of adults or peers without permission being sought
- inappropriate or bullying text messages
- 'happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed
- Sexting- the sending of suggestive or sexually explicit personal images via mobile phones
- Wireless internet access which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.

The school is not responsible for any theft, loss or damage of any personal mobile device.

4.4 Games Consoles

- Staff should be aware that games consoles have Internet access. Before use within school, authorisation should be sought from the Headteacher and e-safety leader. When granted any such activity must be supervised by a member of staff at all times.

4.5 Video-conferencing and webcams

Video conferencing by members of staff is allowed but the Acceptable Use rules still apply. Under no circumstances should a student be engaged in video conferencing unless under the direct supervision of a teacher throughout.

Students need to tell an adult immediately of any inappropriate use by another student or adult.

5. Web 2.0 Technologies

5.1 Managing Social Networking and other such technologies

Social networking sites are proving increasingly popular amongst both adults and young people alike.

The service offers users a public space through which they can engage with other online users. However, as with any online communication with young people, there are a number of risks associated which must be addressed. With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published.

In response to this issue the following measures will be put in place:

- The school will control access to social networking sites through filtering system.

- Students are strongly and regularly advised against giving out personal details or information which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, IM and email address or full names of friends.)

- Staff and students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos which could reveal personal details (e.g. house number, street name, school uniform)

- Staff and students are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.

- Social networking can be a vehicle for cyberbullying. Users are encouraged to report any incidents of bullying to the school allowing for the procedures, as set out in the anti-bullying policy, to be followed.

5.2 Additional social networking advice for staff (Please see Social Media Policy)

Social networking outside of work hours, on non school-issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.

- Staff should not engage in personal online contact with students outside of Headteacher authorised systems (e.g. school email account for homework purposes). This is relevant for all students currently on roll at the school and under 19 years of age.

- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.

- Staff are advised against accepting invitations from colleagues until they have checked with them in person that the invitation is genuine (avoiding fake profiles set up by students)

5.3 – Virtual Learning Environment (VLE)

The school uses a VLE to allow access to a variety of educational resources and opportunity to communicate and share tasks with teaching groups and staff.

Curriculum Team Leaders will monitor their teams section of the VLE. All Staff are responsible for content, contact and conduct whilst using the VLE are they would be in a traditional learning environment.

6. Safeguarding measures

6.1 Filtering

Please refer to the Acceptable Use Rules for Staff and children and young people for the appropriate use of the school systems.

6.2 Tools for bypassing filtering

Web proxies are probably the most popular and successful ways for students to bypass internet filters. Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass the school's security controls (including internet filters, antivirus solutions or firewalls.) as stated in the Acceptable Use Rules.

Violation of this rule will result in disciplinary or in some circumstances legal action.

7. Monitoring

The use of on-line technologies by student and staff is monitored on a regular basis. Teachers should monitor the use of school systems and internet during lessons and also monitor the use of e-mails from school and at home, on a regular basis.

8. School library

The computers in the school library will be protected in line with the school network.

9. Parental Support

As part of the approach to developing e-safety awareness with children and young people, the school offer parents the opportunity to find out more about how they can support the school or setting in keeping their child safe and find out what they can do to continue to keep them safe whilst using on-line technologies beyond school. The School does this through Parent/Carer Information Evenings and via guidance on the school website.

10. Links to other policies

10.1 Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication. People should not treat on-line behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour.

10.2 Managing allegations and concerns of abuse made against people who work with children.

Allegations made against a member of staff should be reported to the designated person for child protection within the school or educational setting immediately. In the event of an

allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

10.3 Citizenship and guidance
The teaching and learning of e-Safety is embedded within the C&G curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line.

10.4 External websites
In the event that a member of staff finds themselves or another adult on an external website, as a victim, then staff are encouraged to report incidents to the Headteacher and unions for advice.

10.5 Disciplinary Procedure for All School Based Staff
In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, then the issue would be dealt with following the school's disciplinary procedures.

11. Appendices

- **Procedure following misuse by Staff**
- **Procedure following misuse by Students**
- **Acceptable Use Rules for Staff, governors and visitors**
- **e-Safety Acceptable Use Rules Letter to Parents/Carer**
- **e-Safety rules for students**

Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the internet, by an adult:

A. An inappropriate website is accessed inadvertently:
   a. Report website to the e-Safety Leader if this is deemed necessary.
   b. Contact ICT Support so that it can be added to the restricted list.

B. An inappropriate website is accessed deliberately or ICT equipment used inappropriately :
   a. Ensure that no one else can access the material by shutting down.
   b. Log the incident.
   c. Report to the e-Safety Leader immediately.
   d. Refer to the Acceptable Use Rules and follow agreed actions for discipline.

C. An adult receives inappropriate material.
   a. Do not forward this material to anyone else – doing so could be an illegal activity.
   b. Alert the e-Safety Leader immediately.
   c. Ensure the material is removed and log the nature of the material.
   d. Contact relevant authorities for further advice if needed.

D. An adult has communicated with a student or used ICT equipment inappropriately:

a. Ensure the child is reassured and remove them from the situation immediately.
b. Report to the Headteacher and Designated Safeguarding Lead immediately, who should then follow Child Protection Policy.
c. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
d. Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff.
e. If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Safeguarding Lead immediately and follow the Allegations procedure and Child Protection Policy.

E. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the e-Safety Leader.

Procedures Following Misuse by Students

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the internet, by students:

A. An inappropriate website is accessed inadvertently:

a. Reassure the student that they are not to blame and praise for being safe and responsible by telling an adult.
b. Report website to the e-Safety Leader if this is deemed necessary.
c. Contact ICT Support so that it can be added to the banned list

B. An inappropriate website is accessed deliberately:

a. Refer the student to the Acceptable Use Rules.
b. Decide on appropriate sanction.
c. Notify the e-Safety Leader, Curriculum Team Leader, Form Tutor and Year Team Leader.
d. Notify the parent/carer.

C. An adult or child has communicated with a student or used ICT equipment inappropriately:

a. Ensure the child is reassured and remove them from the situation immediately.
b. Report to the Headteacher and Designated Safeguarding Lead immediately.
c. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.

d. If illegal or inappropriate misuse the Headteacher must follow Child Protection Policy.
e. Contact the Police as necessary.

D. Threatening or malicious comments are posted about a child or adult in school:

a. Preserve any evidence.
b. Inform the e-Safety Leader
c. Contact the Police as necessary.

N.B. There are three incidences when you must report directly to the police.

- *Indecent images of children found.*
- *Incidents of 'grooming' behaviour.*
- *The sending of obscene materials to a child/student.*

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you could be liable to prosecution and investigation by the police.

Acceptable Use Rules for Staff, Governors and Visitors at Northampton School *for Boys*

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to students before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of students if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Safeguarding Lead or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who the Designated Safeguarding Lead is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact students via personal technologies, including my personal e-mail and should use the school E-mail and phones and only to a student's school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass school filtering systems is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures for staff misuse.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard students when using on-line technologies.

Signed…… . Date……

Name (printed)……

E-Safety / Acceptable Use Rules Letter to Parents/Carer

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing online material. In order to support the school in educating your son about e-Safety (safe use of the internet), please read the following Rules with your son then sign and return the slip.

These Rules provide an opportunity for further conversations between you and your son about safe and appropriate use of the internet and other on-line tools (e.g. mobile phone), both within and beyond school.

Should you wish to discuss the matter further please contact the schools e-Safety Leader.

Yours faithfully,

Mr P Beaumont & Mr M Kneeshaw
Safeguarding Team

E-Safety Acceptable Use Rules Return Slip

Child Agreement:

Name: _____Class:_____

- I understand the Rules for using the internet, E-mail and on-line tools, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____ Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Carer Signature: _____ Date: _____

E-Safety Rules for students

At Northampton School *for Boys* we encourage the use of the ICT resources, including the internet, enabling us to use vast resources, in support of research and education.

As students at Northampton School *for Boys*;

- **We know access to the networked resources is our privilege and used in support of our studies.**

- **We do not access, create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to ourselves and others.**

- **We follow our teacher's instructions carefully.**

- **We must have permission from our parents/carers before we can use the internet for our own independent research at school.**

- **We ask "Is it true?" We do not assume that information published on the Web is accurate or true.**

- **We keep our username and password private. We do not tell anyone.**

- **We are careful about what we write. We check our work before we print or send anything. We do not use bad language. We do not write racist, sexist, abusive, homophobic or aggressive words. We do not write things that could upset and offend others. We could give ourselves and the school a bad name.**

- **We do not ever give personal information about ourselves and anyone else, such as our address, telephone number and private details in an e-mail or on a Website. We know we could put ourselves or others in danger.**

- **We are wise net surfers. We do not go to sites or download any materials, which are offensive, violent and pornographic.**

- **We understand that we are forbidden to use any technology designed to avoid or bypass school filtering controls. We know that these filters are in place to protect us from viewing websites that are unsuitable or unsafe for us.**

- **We will report any incident that breaches the Acceptable Use Policy rules immediately to our teacher.**