Northampton School
for Boys

E-Safety and Acceptable Use Policy

Approved by: NSB Trust Board

Designated Senior Leader:	**Matt Kneeshaw**
Data Controller:	**Aaron Peck**
Data Protection Officer:	**Judicium**

Based on policy developed by the Education Inclusion Partnership Team EIPT, Northamptonshire Police, the Northamptonshire Safeguarding Children's Board, Governors, Parents/Carers and Children, and in partnership with Professional Associates, following Becta Guidelines and review of this policy by Becta.

Contents

1. Acceptable Use Policy and Agreement 4
2. What is an AUP (Acceptable Use Policy)? 4
3. Roles and responsibilities of the school 5
   3.1. Governors, the Headteacher and the Data Controller 5
   3.2. e-Safety Leader 5
   3.3. Adults in school 6
   3.4. Students 6
   3.5. Parents 7
4. Appropriate and Inappropriate Use of School Systems 7
   4.1. By staff 7
      4.1.1. Provision of ICT Systems 7
      4.1.2. Network Access and Security 7
      4.1.3. School Email 7
      4.1.4. Internet Access 8
      4.1.5. Digital Cameras 9
      4.1.6. File Sharing 9
      4.1.7. Mobile Phones 9
      4.1.8. Use of Whatsapp 9
      4.1.9. In the event of inappropriate use 11
   4.2. By Students 11
      4.2.1. In the event of inappropriate use 11
5. The curriculum and tools for Learning 11
5.1. Internet Education 11
   5.2. E-mail use 12
   5.3. Smartphones and other emerging technologies 12
   5.4. Games Consoles 12
   5.5. Video-conferencing and webcams 12
      5.5.1. The use of Video in Microsoft Teams 13
6. Social Networks 13
   6.1. Managing Social Networking and other such technologies 13
   6.2. Official use of social media 13
   6.3. Staff official use of social media 14
   6.4. Additional social networking advice for staff 15
7. Online Communication and Safer Use of Technology 15
   7.1. Virtual Learning Environment (VLE) 15

7.2. Microsoft Teams 16
7.3. Managing the Northampton School for Boys website 16
7.4. School Video & Imagery 16
7.5. Managing email 16
7.6. Official videoconferencing and webcam use 17
8. Safeguarding measures 17
8.1. Filtering 17
8.2. Management of applications (apps) used to record student progress 17
8.3. Tools for bypassing filtering 18
8.4. Classroom Control Software 18
8.5. Security and Management of Information Systems 18
9. Monitoring 18
10. School library 18
11. Parental Support 19
12. Links to other policies 19
12.1. Behaviour and Anti-Bullying Policies 19
12.2. Managing allegations and concerns of abuse made against people who work with children.19
12.3. Personal Development 19
12.4. External websites 19
12.5. Disciplinary Procedure for All School Based Staff 19
13. Appendices 19
13.1. Procedures Following Misuse by Staff 20
13.2. Procedures Following Misuse by Students 21
13.3. Acceptable Use Policy 22
Acceptable Use Rules for Staff, Governors and Visitors at Northampton School *for Boys* 22
E-Safety / Acceptable Use Rules Letter to Parents/Carer 23
E-Safety Rules for students 24

1. Acceptable Use Policy and Agreement

This policy is designed to enable acceptable use for staff and governors.

The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of staff, governors and pupils it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure;
- Define and identify unacceptable use of the School's ICT systems and external systems;
- Educate users about their data security responsibilities;
- Describe why monitoring of the ICT systems may take place;
- Define and identify unacceptable use of social networking sites and school devices; and
- Specify the consequences of non-compliance.

This policy applies to staff members, governors and all users of the School's ICT systems who are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.
The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.
If you are in doubt and require clarification on any part of this document, please speak to the Director of Information Services.

2. 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 Messaging System
- Gaming
- Music Streaming/Downloading
- Smart Tech i.e. smart phones. Watches and TV's.
- 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 and messaging.
- 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

3. Roles and responsibilities of the school:

3.1. Governors, the Headteacher and the Data Controller

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 will appoint a Data Controller who is responsible for data and data security in the school. The Data Controller 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 Data Controller 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.

3.2. 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 Director of Information Services to ensure the security of the school’s network and report any breach or misuse to the Data Controller.
- 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
- Ensure that internal messages within the school Online Messaging system is fit for a professional establishment;
- Tone of e-mails is in keeping with all other methods of communication between staff
- Appropriate and professional conduct is kept at all times when communicating with Students.

3.3. 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(s) 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 Data Controller and IT Support.
- Alert the Data Controller 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 General Data Protection Regulation. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a device/station unattended when they or another user is logged in.
- Report accidental access to inappropriate materials to the Director of Information Services 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.
- Ensure that Messaging and Posting in Team Channels is appropriately used in the schools Microsoft Teams– take care when using the school's messaging system and ensure messages and/or post are appropriately worded as such documents can be accessed through the Freedom of Information Act 2000. Staff should not use MS Teams to contact parents.

3.4. 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 Computer Science lessons and C&G.
- Taught to tell an adult about any inappropriate materials, abuse, misuse or contact from someone they do not know straight away.

3.5. 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.

4. Appropriate and Inappropriate Use of School Systems

4.1. By staff

4.1.1. Provision of ICT Systems

All equipment that constitutes the School's ICT systems is the sole property of the School.
No personal equipment should be connected to or used with the School's ICT systems. Users must not try to install any software on the ICT systems without permission from the Director of Information Services. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.
The Director of Information Service and the Information Services Manager is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptops/desktop computers or ICT equipment may be removed at any time and without prior warning for regular maintenance, reallocation or any other operational reason. Maintenance includes but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

4.1.2. Network Access and Security

Users are not permitted to make any physical alteration either internally or externally, to the School's computer and network hardware.

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created consisting of a username, password and an e-mail address. All passwords should be of a complex nature to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them with any other person, except to designated members of the IS Support Team for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the Director of Information Service or Information Services Manager as soon as possible.

Users should only access areas of the Schools computer systems to which they have authorised access.
When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the School ICT systems or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the School ICT systems or cause difficulties for any other users.

4.1.3. School Email

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.
Where email is provided, it is for academic and professional use with reasonable use being permitted. Personal use should be limited to short periods during recognised break times and comply with this Acceptable Use policy. The School's email system can be accessed from both the School computers and via the internet from any computer. Wherever possible, all School related communication must be via the School email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- 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 a secure method including:
  - Email encryption;
  - A secure upload portal (where by the recipient will be required to log in to retrieve the email/documentation sent);
  - Password protection on sensitive documents. The sender must ensure that the password is sent separately to the intended recipient (i.e., in a separate email or over the phone).
- Emails should not contain children's full names in the subject line and preferably, not in the main body of the text either. Initials should be used wherever possible.
- Access to school/setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g., confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible, emails must not contain personal opinions about other individuals e.g., other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

4.1.4. Internet Access

Internet access is provided for academic and professional use with reasonable use being permitted. Priority must always be given to academic and professional use.

The School's internet connection is filtered meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case, the website must be reported immediately to IS Support Team.

Therefore, staff must not access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.
Misuse of the internet may in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material or using any of the following facilities will amount to gross misconduct (this list is not exhaustive):

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;

- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found, the School may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.
If necessary, such information may be handed to the police in connection with a criminal investigation.

4.1.5. Digital Cameras

The School encourages the use of digital cameras and video equipment. However, staff should be aware of the following guidelines:

- Photos should only have the pupil's name if they are on display in school only. Photos for the website or press must only include the child's first name.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones, iPads or similar.
- All photos should be downloaded to the School network as soon as possible.
- The use of mobile phones for taking photos of pupils is not permitted.

4.1.6. File Sharing

Any files stored on removable media must be stored in accordance with the Information Security Policy, summarised as follows:

- If information/data is to be transferred, it must be saved on an encrypted, password protected, storage device.
- No school data is to be stored on a home computer or un-encrypted storage device.
- No confidential or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

4.1.7. Mobile Phones

Mobile phones are permitted in school with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.

All phone contact with parents regarding school issues will be through the Schools phones. Personal mobile numbers should not be given to parents at the School.

4.1.8. Use of Whatsapp

WhatsApp is not permitted for use on School issued devices or personal devices for School business. Members of staff are able to use WhatsApp on their own devices for personal communication. However,

staff should not communicate internally with other staff members for School business using their personal WhatsApp accounts, sharing School related information which could include categories of personal data.

The School has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the School, staff and students at all times and must treat colleagues, students and associates of the School with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the School's reputation, nor the reputation of individuals within the School are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of the Director of Information Services.
- Members of staff will notify the Director of Information Services if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos which show pupils of the School who are not directly related to the person posting them, should be uploaded to any site other than the School's website.
- No comment, images or other material may be posted anywhere, by any method that may bring the School or the profession into disrepute.
- Users must not give students access to their area on a social networking site (for example, adding a student as a friend on Facebook). If in exceptional circumstances, users wish to do so, please seek advice from Director of Information Services.

The School may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the School's ICT system is or may be taking place or the system is or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the Director of Information Services to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.
Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy or any other school policy;
- investigate a suspected breach of the law, this policy or any other school policy.

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, this includes when using a school device.

4.1.9. In the event of inappropriate use

If a member of staff is believed to misuse the school's IT system or a school device in an abusive or illegal manner, a report must be made to the Director of Information Services and Designated Safeguarding Lead who will liaise with the Headmaster immediately and all appropriate authorities contacted. Misuse may result in disciplinary action being taken against the member of staff concerned.

4.2. 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 displayed when logging into PC's 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, cloud drives 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.

4.2.1. 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.

5. The curriculum and tools for Learning

5.1. Internet Education

Schools and educational settings should teach children and young people how to use the internet safely and responsibly. They should also be taught, through Computer Science and PSHE 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
- Data Privacy
- 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 data uploaded to web sites and e-mailed to other people does not include any personal data.

5.2. E-mail use

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.

5.3. Smartphones and other emerging technologies

Such technologies are not allowed in school for year 7 to 11, with sixth form students allowed access during personal study only and 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 with the use of Virtual Private Networks (VPN's)

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

5.4. Games Consoles

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

5.5. 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 in school 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.

5.5.1. The use of Video in Microsoft Teams

The school is using Microsoft Teams to help deliver online lessons during lockdowns and student absences due to COVID-19. The school has given staff training and expectations on how to conduct themselves while using live video technology. Teachers are expected to:

- Staff MUST Turn off incoming student video feeds
- Staff MUST turn off their camera feed
- Students must mute their microphones during live lessons

6. Social Networks

6.1. Managing Social Networking and other such technologies

Social networking sites/apps are very 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 along side the school Social media policy:

- 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.
- Inappropriate or excessive use of social media during schools hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the Senior Leadership team and will be managed in accordance with existing school policies such as anti-bullying, staff handbook, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

6.2. Official use of social media

- Official use of social media sites by school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.

- Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use school provided email addresses to register for and manage official school approved social media channels.
- Staff running official school social media channels will ensure that they are aware of the required behaviours and expectations of use as in the school Social Media Policy. They will ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official school social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official school social media sites will comply with legal requirements will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by school will be in line with existing policies, including: anti-bullying and child protection and the Social Media Policy.
- Images or videos of students will only be shared on official school social media sites/channels in accordance with NSB School's Photographic Image Use policy.
- Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the NSB's School website and take place with written approval from Senior Leadership Team.
- Senior Leadership Team staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/carers and students will be informed of any official use of social media use, along with expectations for safe use and School action taken to safeguard the community.
- Northampton School for Boys official social media channels are:
    - https://twitter.com/NSBSchool
    - https://twitter.com/NSBExpArts
    - https://twitter.com/NSBSport
    - https://en.wikipedia.org/wiki/Northampton_School_for_Boys
    - https://www.youtube.com/channel/UCFjmlpp4OOZwbiP2kJK_hzA
- An account will link back to school's website and/or AUP to demonstrate that the account is official.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

6.3. Staff official use of social media

- If staff are participating in online activity as part of their capacity as an employee of Northampton School *for Boys*, then they are requested to be professional at all times and that they are an ambassador for Northampton School *for Boys*.
- Staff using social media officially will disclose their official role/position, but always make it clear that they do not necessarily speak on behalf of Northampton School *for Boys*.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within Northampton School *for Boys*, including: libel; defamation; confidentiality; copyright; data protection as well as equalities laws.
- Staff must ensure that any image posted on Northampton School *for Boys* social media channels have appropriate written parental consent.

- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of Northampton School *for Boys* unless they are authorised to do so.
- Staff using social media officially will the Director of Information Services, Northampton School *for Boys* online safety (e-safety) lead and/or the head teacher of any concerns such as criticism, or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with students or parents/carers through social media and should communicate via Northampton School *for Boys* communication channels.
- Staff using social media officially will sign Northampton School *for Boys* AUP and read the Social Media policy before official social media use will take place.

6.4. Additional social networking advice for staff

Social networking outside of work hours, on non school-issue equipment, is the personal choice of all school staff and is not permitted during the working day as set out in the schools Social Media Policy. 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, MS Teams or AIM). 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)

7. Online Communication and Safer Use of Technology

7.1. Virtual Learning Environment (VLE)

- The Senior Leadership team and staff will regularly monitor the usage of Northampton School *for Boys* learning platforms and systems by students and staff in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised about acceptable conduct and use when using Northampton School *for Boys* learning platforms and systems.
- Only members of the current student, parent/carers and staff community will have access to Northampton School *for Boys* platforms and systems.
- All users will be mindful of copyright issues and will only upload appropriate content onto the portal.
- When staff and students leave Northampton School *for Boys* their account or rights to specific Northampton School *for Boys* areas will be disabled.
- Any concerns about content on Northampton School *for Boys* platforms and systems may be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - The material will be removed by the site administrator if the user does not comply.
    - Access to the platforms/systems for the user may be suspended.
    - The user will need to discuss the issues with a member of Senior Leadership team before reinstatement. A student's parent/carer may be informed.

- A visitor may be invited onto the portal by a member of the Senior Leadership Team. In this instance there may be an agreed focus or a limited time slot.
- Students may require editorial approval from staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

7.2. Microsoft Teams

The School uses Microsoft Teams to allow access for students to communicate with their teachers and fellow students during a lockdown situation. This allows live lessons and messaging between Staff and Students for discussion. Please follow the Guidance on the VLE to stay safe with Students: https://vle.mynsb.co.uk/course/index.php?categoryid=461

7.3. Managing the Northampton School *for Boys* website

- Northampton School *for Boys* will ensure that information posted on Northampton School *for Boys* website meets the requirements as identified by the Department for Education (DfE).
- Northampton School *for Boys* will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or students personal information will not be published on Northampton School *for Boys* website without explicit permission.
- The administrator account for the Northampton School *for Boys* will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.4. School Video & Imagery

- Northampton School *for Boys* will ensure that all images are used in accordance with Northampton School *for Boys* Photographic Image Use policy.
- In line with Northampton School *for Boys* Photographic Image policy, written permission from parents/carers will always be obtained before images/videos of students are electronically published.

7.5. Managing email

- Students may only use Northampton School *for Boys* provided email accounts for educational purposes.
- All staff are provided with a specific Northampton School *for Boys* email address to use for any official communication.
- The use of personal email addresses by staff for any official Northampton School *for Boys* business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and/or encrypted methods.
- Members of the Northampton School *for Boys* community must immediately tell a member of the Senior Leadership Team if they receive an offensive communication.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Access in Northampton School *for Boys* to external personal email accounts may be blocked.

- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully before sending, in the same way as a letter written on Northampton School *for Boys* headed paper would be.
- Northampton School *for Boys* email addresses and other official contact details will not be used for setting up personal social media accounts or subscribing to services.

7.6. Official videoconferencing and webcam use

- All videoconferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer.
- Videoconferencing contact information will not be posted publicly.
- Videoconferencing equipment will not be taken off the premises without prior permission from a DSL.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Students will not use, or have access to, videoconferencing equipment without permission

8. Safeguarding measures

8.1. Filtering

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

- Northampton School *for Boys* Governing Body and Senior Leadership Team have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit students' exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the Senior Leadership team; all changes to the filtering policy are logged and recorded.
- The Director of Information Services will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- Staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

8.2. Management of applications (apps) used to record student progress

- The Headmaster is ultimately responsible for the security of any data or images held of students.
- Apps/systems which store personal data will be risk assessed prior to use.
- Personal staff mobile phones or devices will not be used for any apps which record and store student's personal details, attainment or photographs.
- Only Northampton School *for Boys* 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.
- Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

8.3. 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.

8.4. Classroom Control Software

The school uses a system to allow staff to monitor and control access for students when accessing the web technology or PC usage on a school PC.

8.5. Security and Management of Information Systems

- The security of Northampton School *for Boys* Information Systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the Northampton School *for Boys* network will be regularly checked.
- The Director of Information Services will review system capacity regularly.
- The appropriate use of user logins and passwords to access the Northampton School *for Boys* network will be enforced for all but the youngest users.
- All users will be expected to lock devices if systems are unattended.
- Northampton School *for Boys* will log and record Internet use on all Northampton School *for Boys* owned devices.

9. Monitoring

- The use of all school owned 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.
- Data logs of all internet and device usage within school is record and held encrypted for 6 months within school and is only accessible by the Director of Information Service and IT Support Team

Any unauthorised use of the School's ICT systems, cloud-based ICT systems, the internet, e-mail and/or social networking site accounts which the Director of Information Services and the Headteacher considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The School reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

10. School library

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

11. 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.

12. Links to other policies

12.1. 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.

12.2. 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.

12.3. Personal Development

The teaching and learning of e-Safety is embedded within the PD 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.

12.4. 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.

12.5. 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.

13. 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

13.1. 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.

13.2. 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.

13.3. Acceptable Use Policy

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.

As a school user of the network resources/equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the School rules (set out within this policy) on its use. I will use the network/equipment in a responsible way and observe all the restrictions explained in the School Acceptable Use Policy. If I am in any doubt, I will consult the Director of Information Services.
I agree to report any misuse of the network to the IS Support Team. Moreover, I agree to report any websites that are available on the School internet that contain inappropriate material to the Director of Information Services. Finally, I agree to ensure that portable equipment such as cameras, tablets or laptops will be kept secured when not in use and to report any lapses in physical security to the Director of Information Services.

- 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 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.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the School will monitor communications in order to uphold this policy and to maintain the School's network (as set out within this policy).

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 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

Acceptable Use Policy for Students

The use of the School's ICT resources and services is a facility granted to students at the School's discretion. This Acceptable Use Policy is designed to ensure appropriate use of devices and the School's networks as well as ensuring students can benefit from using the School systems.

Use of the School network constitutes agreement to comply with this policy.

These rules apply to a student's use of the School network, whether using School computers or devices or using their own devices as a method to log in. This also applies to accessing the School network off site.

Students are given a user account to enable them use of the network and by continuing to use the network, users must abide by the following:

Student Terms of Use

- You are responsible for account access on the School network. Any unauthorised use of your account should be flagged to the School's ICT team immediately.
- Use of the School network is regularly monitored by the School's ICT team (which includes email access). The School will monitor any traffic over the School system to prevent threats to the School's network.
- You must not use someone else's username to gain access to the School network.
- You should not write down or share your password with anyone else.
- You are not permitted to share access details to the School's network or Wi-Fi password with anyone else.

- You must not attempt to circumvent security of any host, network or account, or penetrate security measures ("hacking") on or accessed through the School network.
- You must not probe, scan or test the vulnerability of the network or other networks.
- You must not try to install any software on School systems without permission from the ICT team. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.
- Any apps or software that are downloaded onto your personal device whilst using the School's network is done at your own risk and not with the approval of the School.
- You must not use the network or your own property to access or process inappropriate materials. This includes (but is not limited to) pornographic material, material which may be seen as violent, offensive or discriminatory, inappropriate text files or files dangerous to the integrity of the network.
- You must not transmit, re-transmit, publish or store material or messages on or through the School network which could be perceived as bullying, threatening, abusive, hateful, indecent, harassing, offensive or defamatory.
- You must report any inappropriate messages or information immediately to the ICT team. This report will help protect other pupils and you.
- You must not record, video or take pictures of other students, staff or third parties whilst using School devices without express permission from a senior member of staff.
- Use of own devices is at the risk of the user. The School cannot accept responsibility for any loss, damage or costs incurred due to use, damage or loss whilst accessing the School's systems.
- Storage media such as USB sticks and hard drives are prohibited at the School.
- Any property owned by students such as mobile phones and iPads may not be used to stream, download or watch videos.
- You may not access the internet except through the School network.
- You must be mindful of the information that you post/share/send online and how this may impact others i.e., you should be kind online.

If a student or user account breaches the above rules, their account may be inspected and their access stopped. A breach may also put you at risk of suspension and/or exclusion.