Northease Manor School

E Safety Policy

Date of review:	**September 2016**
Date of next review:	**September 2017**
Reviewer:	**Designated Safeguarding Lead / E-Safety Coordinator**

Introduction.

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the internet on a daily basis. Access to such technology provides a wide a range of opportunities for learning and social interaction but can place children, young people and adults in danger.

This policy covers issues relating to the safe use of the internet, mobile phones and all computer and tablet technologies, both in and out of school. It includes education for all member of our school community on the risks and responsibilities relating to the use of technology, and is part of the duty of care which applies to everyone working with our students.

This policy applies to all members of Northease Manor School's community, including staff, students, volunteers, parents, carers, and visitors and community users who have access to, and are users of, the school's ICT system, both in and out of the school.

Roles and Responsibilities

1. **Governors.**

The governors are responsible for ensuring that the school complies with its legal obligations. The governors are responsible for the approval of the Technology Policy and for reviewing the effectiveness of the policy. The policy review will be carried out by the Student Welfare Committee of the governing body which will receive regular information about e-safety incidents and monitoring reports. The Safeguarding and Child Protection governor has taken on the role of E Safety governor also.

The role of the E Safety governor will include:

- regular meetings with the E-Safety Coordinator
- regular monitoring of e safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant governors' meetings.

2. Headteacher

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Coordinator.

The Headteacher and the Designated Safeguarding Lead and Behaviour should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues where appropriate.

The Headteacher and the Senior Leadership Team will receive regular monitoring reports from the E-Safety Coordinator.

3. E-Safety Coordinator

- Leads the E Safety Group
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school's technology policies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff, including boarding staff
- Carry out an audit of the e-safety training needs of all staff regularly**.**
- Provides e-safety workshops and literature for parents and carers
- Liaises with the school's technical consultants
- Ensures that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering/ change control logs
- Liaises regularly with the school's Designated Safeguarding Lead
- Reports regularly to the Headteacher and Senior Leadership Team.
- Investigates e-safety breaches and informs the Designated Safeguarding Lead of the incident and investigation for them to review and decide upon any sanction.
- Informs the Designated Safeguarding Lead if any incident raises child protection and safeguarding issues.
- Responsible for ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack,
- Responsible for ensuring that the school meets required e-safety technical requirements
- Responsible for ensuring that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

- Responsible for ensuring that the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Responsible for ensuring that they keep up to date with e-safety technical information in order to carry out their e –safety role effectively, and to inform and update others as relevant
- Responsible for ensuring that the use of the network, internet, remote access and email is regularly monitored in order that any misuse can be reported to the Designated Safeguarding Lead where relevant
- Responsible for ensuring that under the Prevent Duty, any misuse relating to extremism or radicalisation is reported to Designated Safeguarding Lead in their role as the School's Single Point of Contact (SPOC)
- Responsible for ensuring that monitoring software is implemented and updated as agreed with the school's technical consultants.

4. Designated Safeguarding Lead

The Designated Safeguarding Lead is a member of the E-Safety Group and is the School's Designated Safeguarding Lead and SPOC.
They receives regular reports from the E-Safety Coordinator and meets weekly with them to review incident logs and filtering/ change control logs through these roles and attendance at E-Safety Group meetings

The Designated Safeguarding Lead reviews all incidents and the investigation of any breach of e-safety and decides upon any sanction.

5. Head of Boarding

The Head of Boarding will ensure that a log is made of any e-safety breach which takes place during residential time. The equipment used will be quarantined, and the member of SLT on standby informed of the incident.

6. Teaching, Boarding and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of the safe use of technology and e-safety matters and of the school's current technology policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the E-Safety Coordinator for investigation
- all digital communication with parents and carers should be on a professional level and only carried out using the official school system
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the and acceptable use agreements

- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- they are alert to the dangers of students accessing material relating to extremism and radicalisation and report any concerns they may have to the Designated Safeguarding Lead/SPOC.

7. E-Safety Committee

The E-Safety Committee provides a consultative group with responsibility for issues regarding e-safety, monitoring the technology policy, planning and implementing initiatives, evaluating the impact of initiatives.

Members of the E-Safety Committee will assist the E-Safety Coordinator with

- mapping and reviewing the e-safety curricular provision- ensuring relevance, breadth and progression
- monitoring network/internet/ incident logs
- consulting parents, carers and students about e-safety
- organising e-safety workshops for parents and carers
- keeping parents informed of e-safety issues and providing literature where appropriate

8. Students

Students are responsible for using the school's digital technology systems in accordance with the Student Acceptable Use Agreement.

Students:

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

9. Parents

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will

take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and information about e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school

Education- Students.

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of our school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff will reinforce e-safety messages across the curriculum. The e-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum as part of PSHE / other lessons and will be regularly revisited
- Key e-safety messages will be reinforced as part of a planned programme of assemblies, tutor time and school activities
- Students will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, students will be guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Coordinator Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site,
- Parents / Carers workshops
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites and publications.

Education & Training – Staff / Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.)
- The E-Safety Coordinator will receive regular updates through attendance at external training events) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors participate in school training / information sessions for staff. This is of particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / child protection.

Technical – infrastructure / equipment, filtering and monitoring.

It is the responsibility of the school to ensure that our IT consultants carry out all the e-safety measures that would otherwise be the responsibility of the school.

Our IT consultants are fully aware of our E-Safety Policy / Acceptable Use Agreements.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved

within this policy are implemented. It will also ensure that our IT consultants will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of the school's technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the IT Coordinator) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every academic term.
- The "master / administrator" passwords for the school ICT system, used by the E-Safety Coordinator and school's technical consultants are also available to the Business Manager and kept in a secure place.
- The school's technical consultants are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- A reporting log system is in place for users to report any actual / potential technical incident / security breach to the E-Safety Coordinator .
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- The acceptable use policy defines the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- The acceptable use policy defines the extent of personal use that users (staff / students) and their family members are allowed on school devices that may be used out of school.
- The acceptable use policy forbids staff from downloading executable files and installing programmes on school devices.
- The acceptable use policy defines the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- The Director of Operations is the Senior Information Risk Officer (SIRO) and Information Asset Owner (IAO)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Students			
	Not Allowed	Allowed	Allowed at certain times (Break times only)	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times (Break times only)	Allowed with staff permission
Mobile phones may be brought to school		✓				✓		
Appropriate use of mobile phones in lessons (With Permission from the teacher)		✓				✓		
Use of mobile phones in social time		✓				✓		
Taking photos of other students on personal mobile phones / cameras / other personal devices)	✓				✓			
Taking photos to support learning (not including students) eg instructions on white board		✓			✓			
Taking photos on school mobile phones / cameras (or using school data card)		✓						✓
Use of other mobile devices eg tablets, gaming devices			✓				✓	
Use of personal email addresses in school, or on school network for non-school related purposes			✓		✓			
Use of personal email addresses in school, or on school network for school related purposes	✓				✓			
Use of school email for personal emails	✓				✓			
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / former students	✓				✓			
Use of messaging apps/ social media on personal devices – not to include contacting students/former students			✓		✓			

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the school service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the E-Safety Coordinator the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications. Under no circumstances should staff use personal email addresses, text messages or social media (including messaging apps) to contact students or former students.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity.

All schools have a duty of care to provide a safe learning environment for students and staff. The school could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Staff training includes acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- no reference should be made in social media to students, parents / carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by E-Safety Coordinator and e-safety committee to ensure compliance with this policy and the Data Protection and Communications Policies.

Unsuitable / inappropriate activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

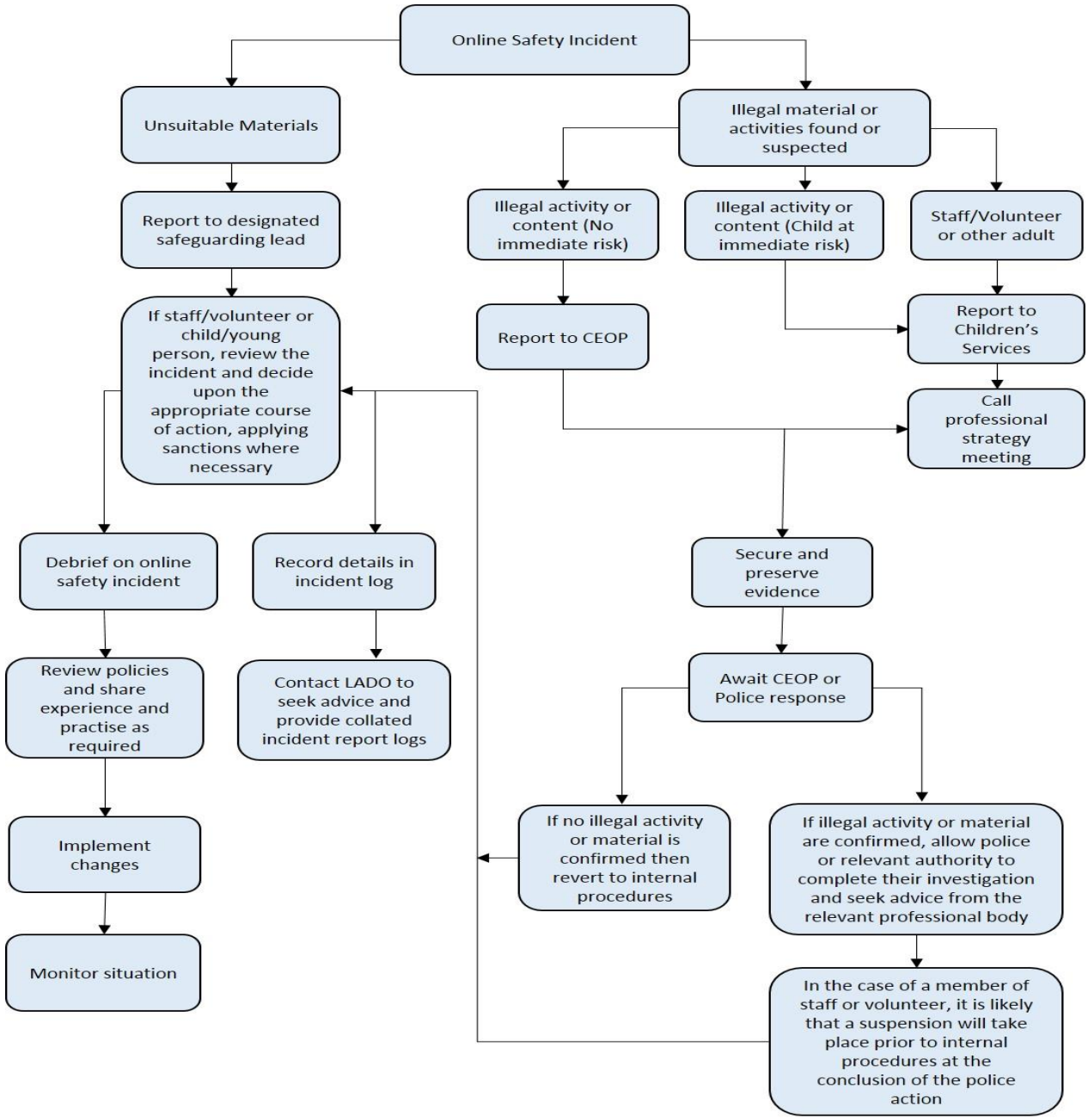
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Accessing extremist websites, especially those with a social networking element.					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			✓			
On-line gaming (non educational)			✓			
On-line gambling					X	
On-line shopping / commerce				✓		
File sharing			✓			
Use of video broadcasting eg YouTube				✓		

Responding to incidents of misuse.

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents.

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents.

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- The E-Safety Coordinator and Designated Safeguarding Lead should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the school will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority Designated Officer (DO).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- The computer in question should be isolated. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for our school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the school for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students — Actions / Sanctions

Incidents:	Refer to IT Coordinator	Refer to Designated Safeguarding Lead	Refer to Headteacher I	Refer to Police	Refer to technical support consultants for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X					
Unauthorised use of non-educational sites during lessons	X	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device		X						X	
Unauthorised use of social media / messaging apps / personal email	X	X						X	
Unauthorised downloading or uploading of files	X	X						X	
Allowing others to access school network by sharing username and passwords	X	X						X	
Attempting to access or accessing the school network, using another student's account	X	X							X
Attempting to access or accessing the school network, using the account of a member of staff	X	X							X
Corrupting or destroying the data of other users	X	X					X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X	X		X
Continued infringements of the above, following previous warnings or sanctions	X	X				X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X		X
Using proxy sites or other means to subvert the school's filtering system	X					X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X						X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X				X	X	X	X

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X				X	X	X
Unauthorised downloading or uploading of files					X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	X	X	X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X			X	X	X	X
Deliberate actions to breach data protection or network security rules	X	X			X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students /former students	X	X	X		X	X	X	X
Actions which could compromise the staff member's professional standing	X	X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X			X	X	X	X
Breaching copyright or licensing regulations	X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Breaches of the E Safety Policy.

By Students.

Any breach of this policy may lead to disciplinary action being taken against the students involved in line with the school's Behaviour Policy.

By Staff.

Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with the school's Disciplinary Policy. A breach of this policy leading to breaches of confidentiality, defamation or damage to the reputation of the school or any illegal acts or acts that render the school liable to third parties will result in disciplinary action appropriate to the severity of the breach

By Contracted Providers of Services.

Contracted providers of services to the school must inform the school immediately of any breaches of this policy by their staff so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school.

B. Mobile Devices.

Years 5, 6, 7, 8 and 9 are not permitted to use mobile phones on school premises during school hours. Boarders in those year groups may use their mobile phones in residential time. Senior School students in Years 10 and 11 are allowed to carry and use their mobile phones appropriately during school hours, as are Years 12 and 13. Staff are also permitted to use their mobile phones during the school day. However, as we are a working community, we need to have regulations governing the use of wi-fi and 3G/4G enabled devices do that incoming communications do not interrupt lessons and so that students use them responsibly and do not disrupt the effective operation of the school.

This policy applies to "standard" mobile phones as well as smart phones such as iPhones, Blackberries, Android and Windows phones, and other 3G or 4G enabled devices such as iPads, iPods, tablets and laptops.

Permitted Use of Mobile Devices.

- When directed by a teacher and within the context of an academic lesson, students may be given permission to use social media. This may be to help students understand the potential or pitfalls of such devices, or to understand better how to use such mediums.
- When directed by a teacher, and within the context of an academic lesson, students may be given permission to video each other or themselves on their own devices.
- There will be occasions when students will want or need to photograph different stages of a project, practical task or experiment. In all cases,

students should seek authorisation from their teacher before using cameras to record their work.

- Under direction from a member of staff, students may use their own personal mobile device to make an appropriate record of their academic work. Staff may withdraw authorisation at any time and students should be mindful of the responsibility given in being allowed to use personal devices. Any images or sections of video which are found to contain images of students, should be deleted at the earliest opportunity.
- No content recorded by a student on a personal device should be uploaded to a social media, video sharing or photograph sharing site without the permission of those being filmed, including members of staff. Doing so could result in disciplinary action.

Non-Permitted Use of Mobile Devices.

- 3G or 4G or wifi enabled devices of any description, including mobile phones, iPods, iPads or tablets must never be taken into public examinations by students or staff.
- Those students who are permitted to use mobile phones should ensure that their phones are off or muted during lessons, unless directed otherwise by the member of staff in charge.
- Students should not be posting updates to social media platforms during the school day unless specifically directed to do so by a member of staff for educational purposes.
- Students should not post information about their specific location or current activity to social media platforms whilst on school trips or in residential time. In doing so, students could affect their personal safety or that of their peers.
- Students should not contact their parents directly when unwell at school, via either phone, social media or electronic methods to arrange to be collected. The student should report to the Student Welfare Officer in the school day or to their houseparent in residential time.
- In the event of an emergency, parents should contact the school office, or houseparent in residential time.
- Under no circumstances should covert recording of lessons take place, or recording take place outside the specific parameters laid out by the member of staff when authorisation is given. Doing so could result in disciplinary action.

Sanctions for Misuse of Mobile Devices.

The school will apply appropriate sanctions to any student or member of staff who uses their mobile phone or other mobile device for bullying, intimidation or for keeping, or disseminating inappropriate texts or images.

Instances of cyberbullying will be punishable in accordance with the school's anti bullying policy and may result in temporary or permanent exclusion, or in disciplinary action in the case of a member of staff.

Dealing with Inappropriate Content on Mobile Devices.

If a member of staff suspects or is informed that a student has inappropriate images on their mobile device, the member of staff will confiscate the device. The Designated Safeguarding Lead will investigate the matter and report to the Headteacher.

Authorised members of staff may investigate the content on the mobile device in line with the school's procedures in relation to Electronic Devices Search and Deletion (See Section C below).

If it is discovered that the student's mobile phone or other mobile device contains inappropriate images of a child or young person (under the age of 18), the Designated Safeguarding Lead as the School's Designated Safeguarding Lead will be informed. The mobile device will remain in the possession of the School's Designated Safeguarding Lead until advice from the Local Authority Designated Officer (DO) and the police has been acted upon. This may include asking all students in possession of the image to delete it; if the image has been forwarded outside the school contact will be made in an attempt to have it removed. The parents of all the students involved will be notified of the situation to ensure all content on devices in the homes of students are removed. In-house counselling will be offered to those concerned.

In the case of staff mobile devices, any instances of inappropriate images of children or young people must be reported immediately to the school's Designated Safeguarding Lead.

Use of Mobile Devices: Staff Guidelines for Photographs and Videos.

Staff should not photograph or video students with a personal mobile digital device unless using the school data card held by the E-Safety Coordinator.

Staff must under no circumstances ever use any photographs of students for anything other than strictly professional purposes. They must never upload photographs or videos of any students on to the internet or social media sites. The only exception is to use photographs of students, where parents have given consent, on the school's own website or other school managed social media platforms.

Parents must give permission for a student's photograph to be used before the photograph is printed in any external publication, such as a local or national newspaper.

Security of Mobile Devices.

The school does not accept responsibility for mobile phone devices or entertainment systems.

Parents are informed that mobile phones and other such devices are not covered by the school's insurance policy.

Staff are advised to keep valuables on them at all times, or keep them in the staff room, thought their security there cannot be guaranteed.

Mobile Device Guidelines for Students.

1. All devices are brought into school at the student's own risk and the responsibility for their safekeeping lies with the student. The school will take no liability for loss or damage.
2. School is a place of work. Students' mobile phones/devices must be switched off (or in silent mode) at all times whilst on school premises, unless specifically authorised by a member of staff.
3. If the use of a device is permitted or directed in a lesson (eg as a calculator, camera or voice recorder) it will be under explicit staff supervision, and permission can be withdrawn at any time.
4. Any student found using a device on school premises without staff permission will receive a sanction.
5. If a student needs to contact home in an emergency, they must speak with a member of staff who will deal with the matter. Students should not contact home in the case of illness, this should only be done by a member of staff.
6. If parents need to contact students in an emergency, they should contact the school office or houseparent if in residential time, and a message will be taken to the student.
7. Parents are reminded that students should not have their mobile devices turned on whilst on school premises and therefore will not be able to check for messages or texts.
8. Students may only access the internet through the school's network; no independent access is permitted (eg via 3G) unless written parental permission has been given in accordance with the school's Digital Media and Independent Access to the Internet Policy. The accessing or updating of social media platforms is not permitted unless it is part of a structured educational activity.
9. Students should be aware that under no circumstances should they enter an examination venue with a device, even if it is switched off. To do so will lead to disqualification from that examination and potentially other examinations.
10. Students should be aware that the use of all devices on school premises is subject to the school's Student Acceptable Use of Technology Agreement.
11. Boarding students have access to their mobile phones after school activities until lights out. All mobile phones are then handed to boarding staff for safekeeping overnight. The phones are then returned to boarding students after breakfast the following morning.

Mobile Device Guidelines for Staff.

1. Staff personal mobile digital devices should be switched off (or on silent mode) during lessons, or at times when they are responsible for the supervision of students.
2. Staff should not use a personal mobile digital device during lessons or when supervising students to receive or make personal calls, receive or send texts or post content to social media platforms.

3. If a member of staff feels that it is necessary to be available to receive a personal call or text on a personal mobile device during a lesson, for which there may be exceptional circumstances, they should explain this to their line manager in advance.
4. Staff should not use a personal mobile digital device during lessons (or when supervising students) to access online resources, emails, apps or similar unless it is considered that the outcome is essential to student learning and cannot be sourced through the school network (in which case, students should be made aware that the mobile device is being use for this educational purpose).
5. Staff should not photograph or video students with a personal mobile digital device unless using the school data card held by the E-Safety Coordinator.
6. Staff should endeavour to make any personal calls on their own mobile telephone in a discreet fashion and away from any student area.
7. Staff should not give out their personal mobile phone numbers or other communication contact information to students. School mobiles must be used at all times and are obtained from the Business Manager.
8. Staff should not use personal email or social media accounts, messaging apps, texts or personal mobile or landline telephones to contact students or former students.
9. Inappropriate use of mobile devices is a serious offence; cases of misuse could lead to disciplinary action being taken against the individual concerned.

C. Electronic Devices: Search and Deletion.

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the internet on a daily basis. Access to such technology provides a wide a range of opportunities for learning and social interaction but can place children, young people and adults in danger. Students are allowed to bring mobile phones and other personal electronic devise to school and use them only within the rules laid out in the sections above relating to mobile devices.

This section relates to what staff should do if they reasonably suspect that the data or file on the device in question has been, or could be caused to cause harm, to disrupt teaching or break the school rules.

Responsibilities.

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data and files on those devices.

Evalynne Charmer – Designated Safeguarding Lead / Head of Boarding
Conchita Landa-Font – E-Safety Coordinator
Martine Carruthers – Deputy Head of Boarding

Members of staff who have been authorised by the Headteacher to carry out searches for and of electronic devices will receive specific training to enable them to judge whether material that is accessed is inappropriate or illegal.

Search.

Authorised members of staff have the right to search such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be caused to cause harm, to disrupt teaching or break the school rules. Whether there are reasonable grounds for suspecting that a student has inappropriate content on their mobile phones is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised to search the content of students' mobile devices.

The authorised member of staff should take reasonable steps to check the ownership of the mobile electronic device before carrying out a search.

The examination of the data/files on the device should go only as far as is reasonably necessary to establish the facts of the incident.

If inappropriate material is found on the device, the authorised member of staff and the Designated Safeguarding Lead should decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police and the DO.

Examples of illegal activity would include:

- Child sexual abuse images (including images of one child held by another child)
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Material relating to terrorism or extremism
- Other criminal conduct, activity or materials.

If the search takes place during residential time, the device should be confiscated by the authorised member of staff and shown to the Designated Safeguarding Lead at the earliest possible opportunity.

Deletion of Data.

Following the examination of an electronic device, if the authorised member of staff and the Designated Safeguarding Lead have decided to return the device to the owner, or to retain it, they may erase any data or files, if they reasonably suspect that the data or file on the device in questions has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

Care of Confiscated Devices.

Members of staff are reminded of the need to ensure the safe keeping of confiscated devices.

Monitoring and Review.

A record should be kept of the reason for the deletion of the data/files. The Designated Safeguarding Lead will ensure that full records are kept of incidents involving the search of mobile phone and electronic devices and the deletion of data/ files. These records will be reviewed by the E Safety Committee half termly.

D. Social Media.

1 INTRODUCTION.

1.1 The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and maintaining pages on internet encyclopaedias such as *Wikipedia*.

1.2 While recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that Northease Manor School staff and contractors are expected to follow when using social media.

1.3 It is crucial that students, parents and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of students and other staff and the reputation of the school are safeguarded.

1.4 Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

2 SCOPE.

2.1 This policy applies to Northease Manor School governing body, all teaching and other staff, external contractors providing services on behalf of the school, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to as 'staff members' in this policy.

2.2 This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school (see sections 5, 6, 7 and Appendices A and B).

2.3 This policy applies to personal webspace such as social networking sites (for example *Facebook*), blogs, microblogs such as *Twitter*, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia,* social bookmarking sites such as *del.icio.us* and content sharing sites such as *flickr* and *YouTube*. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

3 LEGAL FRAMEWORK.

3.1 Northease Manor School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- The Human Rights Act 1998
- Common law duty of confidentiality
- The Data Protection Act 1998.

3.2 Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. student and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School business records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

3.3 Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

3.4 Northease Manor School could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render Northease Manor School liable to the injured party.

4. PRINCIPLES – *BE PROFESSIONAL, RESPONSIBLE AND RESPECTFUL.*

4.1 You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.

4.2 You must not engage in activities involving social media which might bring Northease Manor School into disrepute.

4.3 You must not represent your personal views as being those of Northease Manor School on any social medium.

4.4 You must not discuss personal information on social media about students, school staff and other professionals you interact with as part of your job.

4.5 You must not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations, or the school.

4.6 You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Northease Manor School.

5 PERSONAL USE OF SOCIAL MEDIA.

5.1 Staff members must not identify themselves as employees of Northease Manor School or service providers for the school in their personal webspace. This is to prevent information on these sites from being linked with the school and to safeguard the privacy of staff members.

5.2 Staff members must not have contact through any personal social medium with any student from Northease Manor School unless the student is a family member. Northease Manor School does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them.

5.3 Any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

5.4 Staff members must not have any contact with students' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

5.5 Staff members must decline 'friend requests' they receive in their personal social media accounts from students or former students until they reach 21 years of age.

5.6 Staff members must not communicate with former students through social sites until the former student is aged 21 years, unless the student is a family member.

5.7 On leaving Northease Manor School's service, staff members must not contact our students by means of personal social media sites. Similarly, staff members must not contact students from their former schools by means of personal social media.

5.9 Information staff members have access to as part of their employment, including personal information about students and their family members, colleagues, and other parties and school financial and operational information must not be discussed on their personal webspace.

5.10 Photographs, videos or any other types of image of students and their families or images depicting staff members wearing school uniforms or clothing with school logos or images must not be published on personal webspace.

5.11 School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

5.12 Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the school's IP address and the intervention will, therefore, appear as if it comes from the school itself.

5.13 Northease Manor School logos or brands must not be used or published on personal webspace.

5.14 Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

5.15 Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

6 USING SOCIAL MEDIA ON BEHALF OF NORTHEASE MANOR SCHOOL.

6.1 Staff members can only use official school sites for communicating with students or to enable students to communicate with one another.

6.2 There must be a strong pedagogical or business reason for creating official school sites to communicate with students or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage.

6.3 Official school sites must be created only according to the requirements specified in Appendix A of this Policy. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

6.4 Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

7 MONITORING OF INTERNET USE.

7.1 Northease Manor School monitors usage of its internet and email services without prior notification or authorisation from users.

7.2 Users of Northease Manor School email and internet services should have no expectation of privacy in anything they create, store, send or receive using the school's ICT system.

8 BREACHES OF THE POLICY.

8.1 Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with the school's Disciplinary Policy and Procedure.

8.2 A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Northease Manor School or any illegal acts or acts that render the school liable to third parties may result in disciplinary action or dismissal.

8.3 Contracted providers of Northease Manor School services must inform the Director of Operations immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school. Any action against breaches should be according to contractors' internal disciplinary procedures.

E. Digital Media and Independent Access to the Internet.

Introduction.

Students are encouraged to develop a healthy approach in their use of audio and visual digital media, including on-line web-based content. Such media can provide valuable enhancements to students' academic studies and recreational leisure time, and it is recognised that the use of such resources should be within a balanced provision of teaching, learning and leisure opportunities. Students' understanding of the responsible use of media needs to be fostered so that they develop a mature and critical understanding of what material is appropriate and what material might be recognised as being offensive to themselves or others. We seek to develop students' independent ability to distinguish between appropriate and inappropriate material. This policy considers students' access and exposure to audio and visual media, and to digital content experienced through all relevant technology, including:

- the School's Information Computer Technology (I.C.T.) provision,
- C.D.s,
- D.V.D.s,
- hand-held music-playing devices,
- mobile smart telephones,
- personal, laptop and tablet computers,
- cameras,

- televisions,
- U.S.B. storage devices,
- computer-gaming paraphernalia
- internet-based social media sites,
- internet accessing dongles, independent internet Access Points and personal Boosters for Wireless Coverage (conveying access obtained through another device such as mobile smart telephone).

This list is not exhaustive.

Purposes:

1. To raise students' awareness of the dangers associated with certain types of audio and visual media.
2. To teach students how to use audio and visual media appropriately and safely.
3. To develop students' ability to distinguish independently between appropriate digital and on-line media, and media that is likely to be recognised as being offensive.
4. To protect students, as much as is reasonably possible, from exposure to digital or on-line content that is illegal, offensive, displays or reflects gratuitous violence, or is not appropriate to their age, understanding or experience.

Broad Guidelines:

Advances in technology provide children and young adults with much greater opportunity to access digitally held material that has the potential to cause offence, negatively affect emotions, or create harmful impressions affecting children's perceptions of themselves and others. The School's technical consultants have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of our hardware system, our data and for training our teaching and administrative staff in the use of I.C.T. They monitor use of the internet and emails and will report inappropriate usage to the E-Safety Coordinator and/or Designated Safeguarding Lead. However, students' access to digital material using means other than the equipment provided by the School means that the blocking and barring of access to certain types of media, and the monitoring of students' use of the School facilities must be part of a wider approach to protecting students and developing their understanding and confidence.

- We will not tolerate any illegal material, and will always report illegal activity to the police and/or the Local Child Safeguarding Board (LCSB). If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our anti-bullying policy and strategy.

- The School adheres to guidance published by the relevant licensing authorities for the vending and public-display of digital media, relating to recommended or specified age-restrictions for digital videos, C.D.s, D.V.D.s, computer-games and social networking sites.

School Staff:

- have the responsibility, in association with parents, to develop students' understanding of the possible dangers of inappropriate media content, and to support students in developing an independent ability to recognise and report to staff inappropriate content with which they come into contact;
- will adhere to recommended age restrictions, as displayed by the appropriate licensing authorities, when sharing media content with students. Where, for academic study purposes content with an age-restriction higher than that of the intended audience is deemed by a member of staff to be of value for the students, short clips may be shown to them. In such circumstances, the sharing of the material will be under the direct supervision of a member of staff, and will not include any scenes of graphic violence or sexual activity;
- will monitor, as much as possible without intruding unreasonably on students' privacy, students' use of technology, including the School I.C.T. provision and students' own equipment. Such monitoring is always with a view to protecting children from harmful media content and fostering their understanding of appropriate use of such technology;
- have the power to confiscate from students any equipment they suspect to be used in association with the viewing or experiencing of inappropriate digital media content;
- will, themselves, adhere to the School's 'Staff Acceptable Use Agreement' for the use of I.C.T., and monitor students' use of technology so that they too comply with the agreement..

Students at the School:

- are not permitted to bring into the School, either physically or by means of technology, material which has a specified age-restriction detailing an age that is older than the age of the student;
- are not permitted to share any age-regulated material with students younger than the specified age-restriction. Such sharing includes viewing or listening to the media in the presence or hearing of younger students, or when younger students are in the immediate vicinity, or leaving age-regulated material so that it can be accessed by students younger than the specified age-restriction;
- are expected to demonstrate their ability, appropriate to their understanding, to distinguish between appropriate and inappropriate media content, and to report to a member of staff any material experienced in School that they believe to be inappropriate;
- may not purposefully view or experience inappropriate digital material, including digital or on-line content that is illegal, offensive, displays or reflects gratuitous violence, or is not appropriate to their age, understanding or experience; may not bring to school dongles or access point technology permitting access to the internet independent of the School's I.C.T. provision, without the prior submission of the completed relevant parental permission form: 'Parental Permission Form Use of Equipment Enabling Independent Access to the Internet, Including Mobile Telephones' (available from the E-Safety Coordinator;
- are expected to adhere to the School's 'Student Acceptable Use Agreement for the use of I.C.T.

Parents, guardians and carers of students at the School:

- are asked to ensure they have activated all appropriate parental controls on technology brought to the School by their son or daughter;
- are encouraged to support their son or daughter in developing a confident appreciation for the potential benefits and dangers afforded by digital media content. The School disseminates training to parents from the Child Exploitation and Online Protection (C.E.O.P.) centre and welcomes the opportunity to support parents, guardians and carers in addressing related issues.

Conclusion:

Developing students' own confidence in recognising the potential dangers of digital media content, and in managing their use of technology appropriately, is extremely important. Audio and visual media provide powerful resources for the education and experience of children and adults; engendering an environment which combines protection from harmful content with teaching an understanding of the possibilities and risks is most likely to provide students with the necessary skills to manage their use of technology independently beyond their time at the School.

Signed by ..... Designated Safeguarding Lead
Review date:

This policy should be read in conjunction with:

Safeguarding and Child Protection Policy.
Data Protection Policy.
Behaviour Policy
Anti Bullying Policy
Extremism and Radicalisation Policy