THE NELSON THOMLINSON SCHOOL

E-Safety Policy and
Acceptable Use Agreement (SAUA/CAUA/PAUA) – ICT systems

Signed by Headmaster:

Signed by Chair of Governors:

Reviewed by Behaviour, Safeguarding and Wellbeing Committee: 19 November 2020

Next review date November 2021

The E-safety policy was approved by the *Governing Body on:*	
The implementation of the E-safety policy will be monitored by the:	*Behaviour Safeguarding and Wellbeing Committee*
Monitoring will take place at regular intervals:	*Annually*
The Governing Body will receive a report on the implementation of the E-safety policy at regular intervals:	*A report will be issued annually, retrospectively from the summer term monitoring*
The E-Safety Policy will be reviewed:	*Annually, Summer Term or earlier if situations dictate* *Amended June 2016, September 2016, September 2017, July 2018, September 2018 & December 2018,* November 2019, November 2020
Should serious E-safety incidents take place, the following external persons / agencies should be informed:	*Police, LSCB school Pastoral Staff Head of Year, DPO, Headmaster*

Contents

Key personnel

- Mr M. Beechey is the SMT lead on E-Safety
- Mr D. Murphy is the E-Safety lead governor
- Mrs A. Wilkinson is the GDPR lead governor
- Mrs M. Banks is the NTS designated Safeguarding Lead
- Mr J. Cooper is the Head of Computing Department
- Mr J. Scott is NTS Network manager
- Mr A. Johnson is the Data Protection Officer (DPO)

Policy development

All access to ICT facilities, the internet and social media must be in support of educational activities and appropriate to the aims of the school. The aims of the E-safety policy and Acceptable Use Agreements are to ensure that all staff and students are clear about what constitutes appropriate use of ICT, the internet and social media in achieving E-safety and meeting GDPR regulations.

All students and staff who access the internet or social media from the school site, or using NTS ICT resources when off site, must be aware that they are responsible for everything that takes place on their computers, tablets or mobile phones and that all activity, including use of the internet on computers, may be logged.

The E-Safety policy has been developed with full consultation of staff, students, governors and parents. Consultation with the whole school community has taken place through a range of formal and informal meetings.The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Pupil logs of internet sites visited.
- Internal monitoring data for network activity.
- Surveys / questionnaires of
  - students / pupils.
  - parents / carers.
  - staff.

Roles and Responsibilities

The following section outlines the ICT and E-safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness. Governors will receive regular information about E-safety incidents and monitoring reports. A member of the Governing Body is the E-Safety Governor, this is Mr A Lloyd. The Behaviour, Wellbeing and Safeguarding committee will report on E-Safety matters, whilst matters relating to GDPR will be reported by the Curriculum, Teaching and Learning Committee.

Headmaster and Senior Leaders

The Headmaster 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 Co-ordinator, Mr M. Beechey.

Network Manager / Technical staff

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required E-Safety and GDPR technical requirements.
- that users may only access the networks and devices through a properly enforced password protection policy.
- the filtering policy, is applied and updated on a regular basis.
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation and action.
- that monitoring software / systems are implemented and updated as agreed in school policies.

All staff

All staff are responsible to ensure:

- they have an up to date awareness of E-Safety and GDPR matters and will comply with this document and associated policies and practices.
- they have read, understood and signed the Acceptable Use Agreement (SAUA).
- they report any suspected misuse or problem to the E-Safety Coordinator or DPO for investigation / action / sanction.
- all email communications between pupils and staff should be on a professional level using staff email accounts. Agreed protocols will be agreed regarding staff/pupil email communication (for example during lockdowns). Use of Social media communications such as, but not limited to, Twitter or Facebook should be through closed specified groups.
- E-Safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the Pupil Acceptable Use Agreement (PAUA).
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations where appropriate.

Staff should

- never reveal personal information, wither their own or that of others, such as home address, mobile and home telephone numbers and personal email address.
- always log off/lock the computer when they finish using a computer. Never leave a computer unattended when you are logged on.
- use their school email address for professional use and avoid using it for personal use in order to avoid accusations of misuse of NTS ICT facilities.

- must not use NTS ICT facilities to access inappropriate internet content or for personal financial gain and must only access social networking sites for the purposes of enhancing the teaching and learning experience of students.
- Attend relevant training and Inset events to familiarise themselves with new systems e.g. Microsoft Teams training

The school network, especially SIMS, can allow staff to have access to confidential information about students and staff. Staff must ensure that such information remains confidential at all times. Transmission of sensitive data should be password encrypted.

Health and Safety Co-ordinator

The Health and Safety Co-ordinator is responsible for issuing this policy to employees as part of their induction process.

Pupils and Sixth-Formers

- are responsible for using the school ICT systems in accordance with the Acceptable Use Agreement (PAUA).
- 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 their GDPR rights and responsibilities, such as those relating to the use of mobile devices and digital cameras, especially with regards to 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.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through Parentmail, newsletters, letters, website / VLE. Parents and carers will be encouraged to support the school in promoting good ICT and E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website / VLE and on-line student / pupil records.
- their children's personal devices in the school (where this is allowed).
- The appropriate posting of photos and videos on social media sites

<u>Safety and reporting misuse</u>

Internet access from the school site is filtered and monitored. Access to inappropriate websites will be blocked, either on a website basis or by blocking inappropriate key words or phrases.

Staff must not use any existing personal social media accounts. Staff must set up new accounts specifically for school use and submit the details for registration to the Network Support team.

Any member of staff who suspects misuse of the internet, social media or ICT facilities must report this to their line manager in the first instance. Any serious or potentially illegal misuse of the internet or ICT facilities such as accessing pornography, cyber-bullying and on site use of

internet and school ICT facilities for personal financial gain, or damaging the reputation of NTS through use of social media must be reported to the Headmaster, or, in the case of misuse by the Headmaster, to the chair of Governors. If a child protection issue is suspected a report should also be made to the designated Child Protection Officer.

Usage rules and guidelines

Software

Students and staff must not download or install software, shareware or freeware or install any such software from portable media without first consulting and obtaining permission from the Network Manager.

Purchasing hardware and software

The Network manager should always be consulted before any hardware or software is purchased to ensure that it is compatible with the school network. Failure to do so may prevent this hardware or software being installed on the network.

Sanctions

The misuse of ICT facilities and the internet or social media by staff is a serious issue and may result in disciplinary action being taken. The Headmaster must be informed of all serious misuse of ICT facilities and the internet or social media. The Chair of Governors must be informed if the Headmaster is suspected of such misuse.

Monitoring

Monitoring of staff activity must be authorised by the Headmaster or, in their absence, one of the Deputy Heads.

Policy Statements

Education – Pupils and Sixth-Formers

ICT acceptable use, E-safety and GDPR (**all referred to as E-safety**) should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum.

- A planned E-Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Pupils should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information including 'Prevent' awareness.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement (PAUP) and encouraged to adopt safe and responsible use both within and outside school.
- Where pupils are allowed to freely search the internet, staff should 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 (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. Internet filters can be relaxed by the ICT support team on request.

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, with online training offered.
- All new staff will receive E-safety training as part of their induction programme.
- The E-Safety Coordinator will receive regular updates through attendance at external training events, e.g., CEOP.
- This E-Safety policy and its updates will be presented to and discussed by staff including regular 'Prevent' training drawing on partners and external agencies for support, information and intelligence.

Training – Governors

Governors should take part in E-Safety training / awareness sessions, with 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

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.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- All users (at KS3 and above) will be provided with a username and secure password by the Department who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The Network Manager is 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 (such as child sexual abuse images or incitement of extremist views) is filtered by the broadband or filtering provider.
- All users are able to report any actual / potential technical incident / security breach to the DPO.
- All users must not download or install software without first consulting and obtaining permission from the Network Manager.
- The provision of temporary access is conducted via induction.
- 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.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. *Memory sticks should not contain sensitive data and should be encrypted. Staff should seek assistance from the ICT support team regarding encrypted memory sticks.*
- The Network Manager will monitor any printer discrepancies with regard to security.

General Laptop Use

In order to maintain data integrity and security, laptops supplied to school employees are provided for personal use only under certain conditions. All staff that use laptops need to be aware of the implications of using laptops in an uncontrolled environment, i.e. anywhere outside of the school setting. The conditions need to ensure the integrity of the information held is kept safe at all times, is seen to be secure, and complies with current GDPR regulations.

- Due to the increasing occurrences of viruses no personal software is to be loaded without the permission of the network manager.
- Laptops are provided for schools use only and should therefore not be used by any other user. Use without proper authorisation is expressly forbidden.
- Laptops should not be left unattended in vehicles. Care should be ensured to reduce the risk of damage in transit.
- Do not share your username and password with anyone.
- To ensure optimal performance of the laptop is maintained; altering any of the settings or software is to be avoided.
- Any call charges incurred while using the internet or collecting e-mails outside of school, are to be borne by the employee.
- The use of laptops at home should not compromise the member of staff or the school community as a whole.
- For insurance purposes and to reduce the risk of theft or unauthorised access to the laptop employees must always take reasonable steps to keep the laptop secure, and never leave it where it will be liable to theft. Failure to follow these steps may result in the insurance company charging the school for any claim.
- Passwords should be strong, and preferably, unique to NTS.

Personal Devices Policy

It should be made clear that mobile devices must **not** in any circumstances be used to:

- Send pictures to other pupils or staff that might upset or humiliate the subject or the recipient.
- Send texts to other pupils or staff that might upset or humiliate the recipient or other pupils/members of staff.
- Take photos, record video or voice where this is then used to cause distress to others e.g. publish this on social media for malicious purposes

*the term personal devices include (but is not restricted to) mobile phones, Kindles, tablets, i.e., any device that is capable of being used to send messages, data, photos, etc.

In order to protect both pupils and staff, the school insists that staff personal mobile phones are not used to communicate with pupils (unless in exceptional circumstances). School mobile phones are available for this purpose (e.g., for use on school trips).

Where a pupil does bring a mobile phone to school, the phone must remain switched off during lesson time. If a phone is heard or seen to go off, it is to be confiscated until the end of the school day. The only exception to this would be in an emergency or with the express approval of a member of school staff. Mobile phones are not permitted to be used in between lessons after period 1 and period 4.

If there is a concern that a device contains inappropriate material that is being used for bullying or may have safeguarding and behaviour concerns, the SMT and/or Pastoral Team have the authority to check the content. This has to be undertaken with another staff member to act as a witness. Appropriate action will then be taken having regard to the Behaviour Policy.

The table overleaf identifies how the school currently considers the benefit of using these technologies for education outweighing their risks / disadvantages.

	Staff and Other Adults				Pupils			
Communication Technologies	Not Allowed	Not Recommended	Allowed	Allowed for Selected Staff	Not allowed	Allowed	Allowed at Certain Times	Allowed with Staff Permission
Mobile phones may be brought to school			✓			✓		
Use of mobile phones in lessons for educational purposes For personal use	✓		✓		✓			✓
Use of mobile phones in social time. Not between lesson changeovers for pupils.			✓			✓		
Taking photos on mobile phones / cameras			✓			✓		
Use of other mobile devices e.g., tablets, gaming devices in social time			✓			✓		
Use of personal email addresses in school, or on school network			✓			✓		
Use of school email for personal emails	✓				✓			
Use of messaging apps for school business			✓			✓		
Use of social media-specific education purpose				✓ *		✓ *		
Use of blogs			✓			✓ *		

*To protect staff this needs to be set up and agreed with the network manager who will be a member of the group. Communication between staff and pupils using school email addresses is monitored using the schools monitoring and filtering systems

Use of digital and video images

Staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet.

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 pupils 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 e.g., on social networking sites.
- In accordance with guidance parents / carers are welcome to take videos and digital images of their children at school events for their own personal use.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution, storage and publication of those images. Cameras can be borrowed from the ICT Department.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images and will have obtained appropriate consent. Consent can be withdrawn at any time.

Parents / carers are requested to sign the permission form in the start of year pack of information issued to parent/guardians to allow the school to take and use images of their children and for the parents / carers to agree. From Year 9 upwards, this consent is sought from the child, as per their right under GDPR.

Data Protection

Personal data will be recorded, processed, transferred and made available according to GDPR regulations which are laid out in full in the NTS GDPR policy (available via the school website).

Communications

All access to ICT facilities, the internet and social media must be in support of educational activities. This is to ensure that all staff are clear about what constitutes appropriate use of ICT, the internet and social media.

All students and staff who access the internet or social media from the school site, or using NTS ICT resources when off site, must be aware that they are responsible for everything that takes place on their computers, tablets, mobile phones and that all activity, including any internet activity, may be logged.

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 and pupils should therefore use only the school email service to communicate with others using the established group email system.
- Users must immediately report to the E-Safety Officer or appropriate person– in accordance with the school policy, 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 pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content. Communications between staff and students may only take place on official school group email systems. Personal email addresses, text messaging or personal social media must not be used for these communications. Communication using social media accounts between staff and students should use closed accounts agreed by the Network manager.

- Any serious or potentially illegal misuse of the internet or ICT facilities such as accessing pornography, cyber-bullying and on site use of internet and school ICT facilities for personal financial gain, or damaging the reputation of NTS through use of social media must be reported to the Head Teacher.
- Staff must not use any existing personal social media accounts to communicate with pupils. Staff must set up new accounts specifically for school use and submit the details for registration to the ICT support manager who will automatically become a member of that account.
- Staff should never reveal personal information, with their own or that of others, such as home address, mobile and home telephone numbers and personal email address.

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the school through limiting access to personal information. School staff should ensure that when using personal social media that:

- 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 or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The misuse of ICT facilities and the internet or social media by staff is a serious issue and may result in disciplinary action being taken. The Headmaster must be informed of all serious misuse of ICT facilities and the internet or social media. The Chair of Governors must be informed if the Headmaster is suspected of such misuse.

User Actions

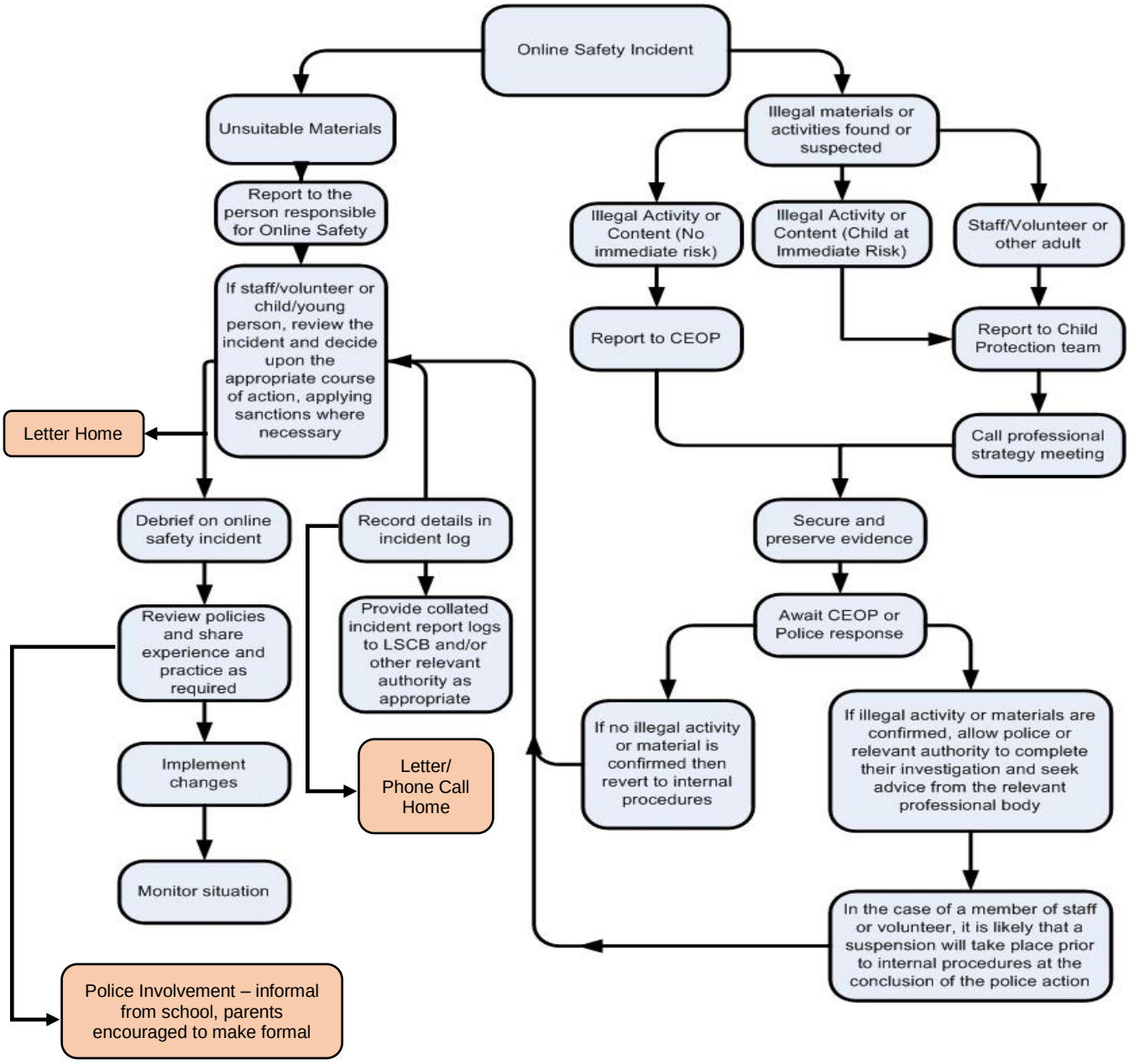
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse 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
	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 (e.g. 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)		X				
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce					X	
File sharing such as Drop box, Google drive and Evernote				X		
Use of social media				X		
Use of messaging apps				X		
Use of video broadcasting e.g. You tube. Staff should pre-watch all clips prior to showing		X				

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.



Electronic Devices - Searching & Deletion Policy

Introduction

Staff laptops owned by the school can be audited at any time or as part of the routine maintenance work. If required, the Headmaster can authorise members of staff to undertake searches of electronic devices.

Responsibilities for searches

The Headmaster has authorised the ICT Technicians, SMT members and Pastoral HoYs to carry out searches for and of electronic devices and the deletion of data / files on those devices. In the sections below they refer to the "authorised staff".

Search

All staff have the right to ask pupils to get out a personal device when asked to do so.
Authorised staff have the right to search the content of an electronic device where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item.
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for especially if this presents a child protection or safeguarding issue.

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a student / pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

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

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g., an occupied classroom, which might be considered as exploiting the student / pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the student / pupil being searched; and there must be a witness (also a staff member) and they should always be the same gender as the student/pupil being searched.

Extent of the search:

The person conducting the search may not require the student/pupil to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
'Possessions' means any goods over which the student/pupil as or appears to have control – this includes desks, lockers and bags.

A student's/pupil's possessions can only be searched in the presence of the student / pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

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. Any further intrusive examination of personal data may leave the school open to legal challenge.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they request a child to 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. 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.
- Inciting extremist views
- other criminal conduct, activity or materials.

Deletion of Data (non-GDPR)

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e., the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Staff should contact the Pastoral Deputy and DPO in the event of this.

Details of such instances will be recorded on the SIMS behaviour log.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices.

Audit / Monitoring / Reporting / Review

The Pastoral Deputy and HoYs will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

Appendices

FORMS

- Student/Pupil Acceptable Use Agreement (PAUA)
- Parents/Carers Acceptable Use Agreement (CAUA)
- Staff and Volunteers Acceptable Use Agreement (SAUA)

Student/Pupil Acceptable Use Agreement (PAUA)

This Acceptable Use Agreement reflects school policy and is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, and personal use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger" when I am communicating on-line including those inciting extremist views.
  I will not give out or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to my teachers

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have the permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will be polite and responsible when I communicate with others.
- I will not take or give out images of anyone and use these images to upset or hurt anyone

I recognise that the school has a responsibility to maintain the security of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to interfere with the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software.

- I will not install or attempt to run programmes of any type on any school device, nor will I try to alter computer settings.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I may face serious consequences. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access **cannot** be granted to school systems and devices.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school).
- I use my own devices in the school using the school network (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil	
Form	
Pupil signature	
Date	

Parent / Carer Acceptable Use Agreement (CAUA)

Your child has signed an Acceptable Use Agreement relating to ICT systems, E-safety and GDPR (all known simply as 'E-safety'). Please support us in discussing this with them and supporting us with the following:

The Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of E-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Student/Pupil Acceptable Use Agreement (PAUA) is in the front of the pupils' planners, so that parents / carers will be aware of the school's expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Pupil Name | Tutor Group

As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I understand that my son / daughter will **not** be allowed access to the school network if they do not sign the Pupil Acceptable Use Agreement (PAUA).

Signed | Date

Staff (and Volunteer) Acceptable Use Agreement (SAUA)

This Acceptable Use Agreement is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed E-Safety in my work with young people including my 'Prevent' duty.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- Will report damaged equipment to the ICT support staff and will not attempt to repair any damage.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. If my personal device is used to record images this should be transferred to school systems and deleted from my device as soon as is practicable
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems.
- I will not engage in any on-line activity that may compromise my professional responsibilities or be harmful to the reputation of the school.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not use personal email addresses when communicating with pupils and parents.
- I will not try to upload, download or access any materials which are illegal (including but not restricted to child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer and understand that all software should be appropriately licenced.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that the GDPR policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential.
- I will immediately report any damage or faults and loss of data to an appropriate person.

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
  - I understand that the laptop allocated to me by the school is for my sole use. I will not let anyone else use my staff laptop, even under supervision
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date