E-SAFETY AND DATA POLICY AND ACCEPTABLE USE POLICY

Background/Rationale

Concerns can be raised with the Designated Safeguarding lead Mrs Hastings-Smith – nsmith@stdominicsgrammarschool.co.uk

Or the network manager – Mr James bnjames@stdominicsgrammarschool.co.uk

Telephone number – 01902 850248

The policy below takes into account KCSIE 2025. Actioned September 2025.

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school.

The internet and other digital and electronic information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communication technologies appropriately and safely, is addressed as part of the wider duty of care to which all who work in schools are bound. St. Dominic's Grammar School E-Safety Policy will help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distributing of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person
- Access to material that might invoke extremist views. Part of this is covered in the **PREVENT** strategy

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety Policy is used in conjunction with other school policies (e.g. Behaviour, Anti-Bullying, and Child Protection Policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience and understanding to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with such risks.

The school has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy

Our E-Safety Policy has been written by the school, on government guidance. It has been agreed by the senior management and approved by Governors. To be followed by everyone including visitors and contractors who intend to use the internet enabled devices within the school premises, whether or not connected to the school's system.

Communication with the whole school community takes place through the following:

- Staff meetings/INSET
- School Council
- Governors meetings/Sub Committee meetings
- School website/newsletters
- School assemblies

Schedule for Development/Monitoring/Review

This E-Safety Policy was approved by the Governing Body on:	September 2021
The implementation of this E-Safety Policy will be monitored by the:	HOF/SLT ICT Network Manager
Monitoring will take place at regular intervals:	Annually
The E-Safety Policy will be reviewed annually, or more regularly if there are any significant new developments in the use of the technologies, new threats to e-safety or incidents that	September 2025
have taken place. The next anticipated review date will be:	
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding Officer Police

The school will monitor the impact of the Policy by using:

- Logs of reported incidents
- Internal monitoring data for network activity

Scope of the Policy

This Policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspection Act 2006 empowers Heads to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this Policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents/carers of incidents of inappropriate esafety behaviour that takes place out of school.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

Headmaster and Senior Leaders

- The Headmaster is responsible for ensuring the safety (including e-safety) of members of the school community but not overall responsibility, though the day to day responsibility for e-safety will be delegated to the ICT Network Manager who liaises with the Senior Leadership Team on e-safety matters.
- The Headmaster/Senior Leaders are responsible for ensuring that the ICT Network Manager and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The ICT Network Manager reports any e-safety issues to the Senior Leadership Team.
- The Headmaster and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Designated Safeguarding Lead

- Has overall responsibility for E-Safety at the school as per KCSIE September 2025.
- 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.
- Liaises with school ICT Network Manager.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments as is responsible for online safety.
- Attends relevant meetings of committee of Governors when required.

- Reports regularly to the Senior Leadership Team.

ICT Network Manager/Technical Staff

The ICT Network Manager is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the e-safety technical requirements outlined in the Acceptable Usage of ICT Network Policy and the E-Safety Policy.
- Users may only access the school's networks through a password procedure, in which passwords are regularly changed.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network, Virtual Learning Environment (VLE), remote access, email, is regularly monitored in order that any misuse/attempted misuse can be reported to the ICT Network Manager and Head of School.
- That monitoring software systems are implemented and updated regularly.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school ESafety Policy and practices.
- They have read, understood and signed the school Staff Acceptable Use of ICT Network Policy.
- They report any suspected misuse or problem to the ICT Network Manager for investigation.
- Digital communications with pupils (e-mail, Virtual Learning Environment (VLE), voice) should be on a professional level and only carried out using official school systems.
- Pupils understand and follow the school E-Safety and Acceptable Use Policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of e-safety issues related to use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- In lessons where internet use is pre-planned, pupils 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.
- Where pupils are asked to research using the internet, a list of pre-checked web-sites should be given if appropriate.

Designated Person for Child Protection. Designated Safeguarding Lead

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data

- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (NB in Pre-Preparatory it would be expected that parents/carers would sign on behalf of the pupils).
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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.

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy
- Accessing the school website in accordance with the relevant school Acceptable Use Policy

Policy Statements

Education – Pupils

The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. 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 education will be provided in the following ways:

- **A planned e-safety programme should be provided as part of ICT and be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities**

- **Pupils should 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**
- **Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school**
- **Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **Rules for use of ICT systems/internet will be posted in all rooms**
- **Staff should act as good role models in their use of ICT, the internet and mobile devices**

Education – Parents/Carers

Many parents and carers have a growing 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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, website
- Parents' Evenings

Education and Training – Staff

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 and online safety training will be made available to staff. An audit of the e-safety training needs of all staff is carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies. Para 62 KCSIE September 2020.
- This E-Safety Policy and its updates are presented to and discussed by staff in staff/ team meetings/Inset days.
- The ICT Network Manager and Head of Senior School will provide advice/guidance/training as required to individuals as required.

Training – Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub committees/group involved in ICT/esafety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/AGBIS/Local Grid for Learning or other relevant organisation.
- Participation in school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is a safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the esafety technical requirements outlined in the Acceptable Use Policy and any relevant E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Network Manager and will be reviewed, at least annually.
- All users (at Preparatory and above) will be provided with a username and password by the ICT Network Manager, who will keep an up to date record of users and their usernames. Users will be required to change their password annually.
- The "master/administrator" passwords for the school ICT system, used by the ICT Network Manager must also be available to the Head of School and kept in a secure place (e.g. school safe).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering system provided by RM plc.
- The school has provided enhanced user-level filtering through the use of the RM Safety Net Universal filtering programme.
- In the event of the ICT Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headmaster.
- Any filtering issues should be reported immediately to the ICT Network Manager.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Network Manager and the Headmaster. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the SLT.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity.
- An appropriate system is in place for users to report any actual/potential e-safety incident to the ICT Network Manager and Senior Leadership Team.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Guest user type is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.

- An agreed policy is in place (see AUP) regarding the downloading of executable files by users.
- An agreed policy is in place (see AUP) that forbids staff from installing programmes and states guidance regarding the use of removable media (e.g. memory sticks/CDs/DVDs) on school workstations/portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Information brought into the school outside the school WIFI cannot be controlled eg. 5G/4G mobile phones

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

It is recognized that with advancement of 3G and 4G that material can be accessed by students. Whilst some filters provided by the school will minimize the majority of inappropriate content it is recognized that not all can be accounted for. The teaching in lessons of PSHE and within the computing science curriculum and external bodies will emphasise what is deemed appropriate or not. Close monitoring of use of mobile phones inparticular for younger students will be maintained. If it felt that children are in breach, measure will be put in place to ensure inappropriate content will not be downloaded and the school reserves the right of total confiscation. This relates to new legislation KCSIE September 2025.

- In lessons where internet use is pre-planned, it is best practice that pupils 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.
- Where pupils are allowed to freely search the internet, e.g. using search engines, 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, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request this by filling in a site allowed form, available from the ICT Network Manager, who 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, and the Head of School informed.
- Pupils should 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video games – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 and tagging them.
- Staff 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will be used anywhere on a website or blog, particularly in association with photographs. Good practice would suggest the use of first names only.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website. If unsure, please refer to the Headmaster's office.
- Pupils' work can only be published with the permission of the pupil and parents or carers.

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

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. A Data Protection Policy is available in **Section B of the Staff Handbook – General Policies and Procedures – Appendix and incorporates GDPR May 2018**

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, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected (many memory sticks/cards and other mobile devices cannot be 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 communication 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:

	Staff and other adults			**Students/Pupils**				
Communication Technologies	Allowed	Allowed at certain	Allowed for selected	Not Allowed	Allowed	Allowed at certain	Allowed with staff	Not Allowed
Mobile phones may be brought to school	√					√	√	
Use of mobile phones in lessons				√				√
Use of mobile phones after school only	√				√ post 16 (lunch & break only)			√
Taking photos on school camera and image capturing devices		√				√		
Use of hand held devices e.g. PDAs, PSPs	√				√ post 16 only			
Use of personal e-mail addresses in school, or on school network				√				√

Use of school e-mail for personal e-mails				√				√
Use of chat rooms/facilities				√				√
Use of instant messaging				√			√	√
Use of social networking sites				√			√	√
Use of blogs				√			√	√

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

- The official school e-mail service may be regarded as safe and secure and is monitored. Staff and students/pupils should therefore use only the school e-mail service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users are aware that e-mail communications may be monitored
- Users must immediately report to the ICT Network Manager; in accordance with the school policy, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail
- Any digital communication between staff and pupils or parents/carers (e-mail, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or public chat/social networking programmes must not be used for these communications
- Pupils are taught about e-mail safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write e-mails clearly and correctly and not include any unsuitable of abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or disturbing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. cyber bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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 certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & 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 sex abuse images					√
	Promotion or conduct of illegal acts e.g. under the child protection, obscenity, computer misuse and fraud legislation					√
	Adult material that potentially breaches the Obscene Publications Act in the UK					√
	Criminally racist material in the UK					√
	Pornography				√	√

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & 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:	Promotion of any kind of discrimination				√	√
	Promotion of racial or religious hatred				√	√
	Threatening behaviour, including promotion of physical violence or mental harm				√	√
	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				√	
Using school systems to run a private business					√	
Use systems, applications, websites or other mechanisms that bypass the filtering of other safeguards employed by SWGfL and/or the school					√	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					√	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					√	
Creating or propagating computer viruses or other harmful files					√	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet					√	
On-line gaming (educational under staff supervision)		√				
On-line gaming (non educational)					√	
On-line gambling					√	
On-line shopping/commerce (for educational purposes only) (staff only)				√		

File sharing (staff only)	√				
Use of social networking sites				√	
Use of video broadcasting e.g. YouTube (staff only)			√		

Reporting

Any users, stakeholders, parents and staff are asked to report any online content that could be offensive and against the standards expected at St. Dominic's Grammar School. Also, incidents where individuals have abused online activity by causing offence. This must be brought to the attention of the ICT Manager and/or the Designated safeguarding lead by contacting the school (see school contact details).

Policy review date: September 2026

Acceptable Use Policy (AUP) Staff and Volunteers

Code of Conduct

Access to the School network is provided for you to carry out recognised school work and extra-curricular activities, but ONLY on the condition that you agree to follow this code of conduct.

General

- All files, including e-mail, held on the network shall be treated as school property. The ICT Network Manager and Headmaster can reset/update user password and examine any file or e-mail without your consent to ensure that the system is being used responsibly. You should not expect that any work or e-mail held on the school's servers will be private.

- As a network user, you are responsible for all aspects of your specific user account on the school network.

- Never reveal your password to anyone, nor let anyone use your account. If you think someone has discovered your password or is using your account, tell the ICT Network Manager or Headmaster immediately. Never use or attempt to use another person's account. The school keeps an audit trail of all network and internet activity and can be traced to individual user and workstation.

- You must not install, or attempt to install, any program(s) on a school computer or attempt to run any from any storage device without the express permission of the ICT Network Manager.

- You must not attempt to by-pass any network security systems, modify any profile or install registry entries.

- Always make sure that you have completely logged off from a computer before leaving it.

- Please leave your computer area and the surroundings as you would like to find them; free of any rubbish or paper.

- No computer equipment or peripherals may ever be removed from its location or tampered with. Any such interference with school property is a most serious offence.

- "Hacking" i.e. unauthorised access or use of personal information, contrary to the provisions of the Data Protection Act, is a serious offence under Law. Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files may be considered a criminal offence under the Computer Misuse Act 1990.

- You should also be aware that the unauthorised downloading or copying of software, music etc. contrary to the provisions of the Copyright, Designs and Patents Act 1988, is not permitted.

- The installing, copying or transmitting of obscene material is forbidden and could be considered a criminal offence under the Obscene Publications Act 1959/1964.

- In addition, any material found in your user area which the school considers inappropriate or offensive will be reported immediately and sanctions applied.

- Staff 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.

The Internet and E-mail

- Staff are, by default, given access to the Internet and e-mail. Please remember that access is a privilege, not a right, and that access requires responsibility at all times.
- The Internet is ONLY provided for you to conduct genuine research and communicate with others. All web-sites you visit, or attempt to access, can be recorded, together with the user's details, the computer that was used and the exact time and date.
- Do not use the Internet or e-mail to subscribe to "newsletter" communications using your school e-mail address, or reply to any type of "subscription form". These types of communications are forbidden and you will instantly lose your access to e-mail or to the Internet.
- Check with a member of the ICT Staff or ICT Technical Support personnel before opening **unidentified** e-mail attachments (they may contain computer viruses) or before completing any online or e-mail questionnaires.
- You must never send, display, access or try to access any obscene or offensive material.
- You must not use obscene or offensive language in e-mails. Remember that you are a representative of your school on a global public system – never swear, use vulgarities, make racial comments, or any other inappropriate language. Remember that the school has the right to read all your e-mails.
- You must never harass, insult or attack others through electronic media. Remember that any e-mail you send can be traced. Also, a recipient of an offensive e-mail from you could choose to take legal action against you.
- Never copy and make use of any material without giving credit to the author. Not only would you be infringing copyright, but you would also be guilty of theft.
- Never reveal to anyone on the Internet or by e-mail any personal information i.e. the home address or personal numbers of yourself or other students.

Sanctions

If you violate the Acceptable Use Policy, access to the Internet and e-mail will be denied and you may be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

Acceptable Use Policy (AUP) Pupil

The School has provided computers for use by pupils, offering access to a vast amount of information for use in studies, acting like an enormous extension to the School library and offering great potential to support the curriculum. Also pupils **with permission only** may use other devices such as laptops, tablets or other electronic devices that can connect to the internet

The computers are provided and maintained for the benefit of all pupils, who are encouraged to use and enjoy these resources responsibly, and to help to ensure they remain available to all. Pupils are responsible for good behaviour with the resources and on the Internet just as they are in the classroom or a school corridor. Pupils should remember that access is a privilege, not a right, and inappropriate use will result in that privilege being withdrawn.

Equipment

Programmes of any type must not be downloaded, installed or stored on any of the School's computers unless directed to do so by a member of staff.

Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources is not allowed and will result in computer privileges being withdrawn.

The School's computers are available to use for educational purposes only. Activities such as buying or selling goods are not allowed.

Food and drink is not allowed in the Computing rooms, the Libraries or near computing equipment.

Security and Privacy

To protect work, pupils must not divulge any password details or use another pupil's logon names/passwords.

Pupils **MUST NOT REVEAL** any personal information on the Internet (i.e. home address, telephone number, name of School or picture).

CYBER BULLYING IS A SERIOUS OFFENCE. Other computer users should be respected and not be harassed, harmed, offended or insulted.

To protect their personal security and the systems, pupils should respect the security on the computers and must not attempt to bypass or alter any setting.

Computer storage areas and flash drives can be searched by staff who may review pupils' files and communications to ensure that the system is being used responsibly.

The School keeps a record of all network and Internet activity which can be traced to individual users and workstations.

Internet

Pupils should only access the Internet for study or authorised/supervised School activities.

Only suitable material may be accessed. Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

Pupils should respect the work and ownership rights of people outside the School, as well as other pupils or staff. This includes abiding by copyright laws.

'Chat' activities, social network sites and messaging services are strictly forbidden.

Social networking sites must not be used to display images of the School or staff or include comments that bring the staff, pupils or the School into disrespect or disrepute.

Laptops and iPads

Students are allowed to bring in their own devices to aid their study. These are brought into School at the owner's risk. They must be used in accordance with the Acceptable Use Policy within School and as directed by school staff. These devices can easily store images and video within the School and the owner must take responsibility for these images. It is advisable to delete all such media files when no longer needed. All videoing or taking pictures using such equipment must be authorised by a member of staff. If internet access is required on these devices permission must be gained from the member of staff teaching or supervising them.

Email

When using emails pupils should be polite and appreciate that other users might have different views from their own. The use of strong language, swearing or aggressive behaviour is not allowed. This applies both inside and outside School when communicating with pupils. The School will store and archive emails sent through the school network in order to safeguard all users within the School.

If an email containing material of a violent, dangerous, racist, or inappropriate content is received, pupils should **always report such messages** to a parent.

Should a pupil violate any part of the School's AUP (Acceptable Use Policy) they will be denied access to the School's Internet and be subject to disciplinary action.

Additional action may be taken by the School in line with existing policy regarding School behaviour. For serious violations, suspension or exclusion may be imposed. Where appropriate, police may be involved or other legal action taken.

Any evidence of cyber bullying outside of school will be reported to parents and the police may be involved. Disciplinary action will be taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Student Name: _____ Signature: _____

I have read and understand the above.

Parent/Guardian Name: _____

Signature: _____

Date: _____

Acceptable Use Policy (AUP) Sixth Form

The School has provided computers for use by pupils, offering access to a vast amount of information for use in studies, acting like an enormous extension to the Sixth Form Library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all pupils, who are encouraged to use and enjoy these resources responsibly, and to help to ensure they remain available to all. Pupils are responsible for good behaviour with computing resources and on the Internet just as they are in the classroom or a school corridor. Pupils should remember that access is a privilege, not a right, and inappropriate use will result in that privilege being withdrawn. .

Also pupils **with permission only** may use other devices such as laptops, tablets or other electronic devices that can connect to the internet.

In addition, Sixth Form students have the privilege of bringing their own laptops, mobile phones or other computing equipment, which allows them access to computing resources and the Internet. Please note that this policy covers all these computing devices in addition to the School resources. To maintain the security of the School network, there is no direct access to the network for private devices and all Internet access via the School broadband connection is protected by filtering and firewall.

Equipment

- Programmes of any type must not be downloaded, installed or stored on any of the School's computers unless directed to do so by a member of staff.
- Damaging, disabling, or otherwise harming the operation of School computers, or intentionally wasting resources is not allowed and will result in computer privileges being withdrawn.
- The School's computing devices are available to use for educational purposes only. Activities such as buying or selling goods are not allowed.
- Food and drink is not allowed in the Computing rooms, the Libraries or near computing equipment.
- Pupils are responsible at all times for the use and security of any computing devices they bring into School. The School has no responsibility for these devices and pupils bring them in at their own risk. Pupils should ensure that they are suitably insured for use in School.
- The use of webcams and other digital image-capturing equipment is not allowed on School premises. Pupils must ensure that they disable any such capabilities before bringing computing devices into School.

Security and Privacy

- To protect work, pupils must not divulge any password details or use another pupil's logon names/passwords.
- Pupils **MUST NOT REVEAL** any personal information on the Internet (i.e. home address, telephone number, name of School, picture or any other personal information).
- **CYBER BULLYING IS A SERIOUS OFFENCE**. Other computer users should be respected and not be harassed, harmed, offended or insulted.
- To protect their personal security and the systems, pupils should respect the security on the computers and must not attempt to bypass or alter any setting.
- Computer storage areas, flash drives and emails can be examined by staff who may review pupils' files and communications to ensure that the system is being used responsibly.
- The School keeps a record of all network and Internet activity which can be traced to individual users and workstations.

Laptops and iPads

Students are allowed to bring in their own devices to aid their study. These are brought into School at the owner's risk. They must be used in accordance with the Acceptable Use Policy within School and as directed by school staff. If internet access is required on these devices permission must be gained from the member of staff teaching or supervising them.These devices can easily store images and video within the School and the owner must take responsibility for these images. It is advisable to delete all such media files when no longer needed. All videoing or taking pictures using such equipment must be authorized by a member of staff.

Internet

- Pupils should only access the Internet for study or authorized/supervised School activities.
- Only suitable material may be accessed. Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Pupils should respect the work and ownership rights of people outside the School, as well as other pupils or staff. This includes abiding by copyright laws.
- 'Chat' activities, social network sites and messaging services are strictly forbidden.
- Social networking sites must not be used to display images of the School or staff or include comments that bring the staff, pupils or the School into disrespect or disrepute.

Email

- Sixth Formers are provided with a School email account for uses connected with their education. The use of personal email addresses is not permitted in School or in communications with staff. School email addresses may not be used for personal use.
- When using emails pupils should be polite and appreciate that other users might have different views from their own. The use of strong language, swearing or aggressive behavior is not allowed. This applies both inside and outside
- If an email containing material of a violent, dangerous, racist, or inappropriate content is received, pupils should **always report such messages** to a parent and/or staff.
- **Should a pupil violate any part of the School's AUP (Acceptable Use Policy) they will be denied access to the School's Internet and be subject to disciplinary action.**
- Additional action may be taken by the School in line with existing policy regarding School behavior. For serious violations, suspension or exclusion may be imposed. Where appropriate, police may be involved or other legal action taken.
- Any evidence of cyber bullying outside School will be reported to parents and the police may be involved. Disciplinary action will be taken.

I have read and understand the above and agree to use the school ICT facilities within these guidelines.

I understand that this policy also applies to any ICT equipment I bring into school.

I have read and understand the above and agree to use the school ICT facilities within these guidelines.

I understand that this policy also applies to any ICT equipment I bring into school.

Student Name: _____

Signature: _____

I have read and understand the above.

Parent/Guardian Name: _____

Signature: _____

Date: _____