PRESFIELD HIGH SCHOOL & SPECIALIST COLLEGE

E Safety Policy

Date Ratified: **11th October 2023**

Date for review: **11th October 2024**

Signed:

Chair of Governors

Contents Page

Introduction

At Presfield High School we recognise that our students are particularly vulnerable to the dangers that new technology and in particular the internet offer. We take Internet Safety very seriously and see it as our duty to keep our students safe whilst using technology not only in school but also at home. This includes technology such as computers, mobile phones or games consoles. . This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education' and 'Working Together to Safeguard Children'.

There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning and we embrace this. Presfield High School has made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." New technologies have become integral to the lives of our students both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students 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 use of new technologies can put our students at risk within and outside the school. Many students are capable of accessing the internet independently and therefore are at risk from either deliberately accessing inappropriate material or, due to their level of literacy, accidently accessing harmful sites.

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 / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers Cyberbullying
- Access to unsuitable video
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement including illegal downloading of music or video files
- The use of AI systems such as ChatGPT to generate unsuitable text, images, sound & video
- The potential for excessive use which may impact the social and emotional development and learning of the young person.

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, bullying and child protection and safeguarding). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to these risks.

Network Safety

Presfield High School currently has both a Windows based network (Research Machines) and a GSuite (Google) network managed and monitored by the schools Network Manager with support from the relevant providers.

To aid in monitoring the school utilises a filtering system called netsweeper that deals with content filtering and web threat management by providing various different functions including:

- Content Categorization: Function that categorises internet content using a database of URLs to assign websites to various categories such as adult content, gambling, social networking and more.
- Filtering Policies: Enables the administrator to create policies specific to user groups that block access to previously mentioned categories.
- Real-time Filtering: Function that checks in real time the web pages that users are accessing and can on the fly block access should it match a banned category found within the database.
- Reporting & Monitoring: Gives the administrator the ability to check what websites are being accessed and generate reports that include key data such as how many times it's been accessed and for how long.
- Cyberbullying & Self-Harm Prevention: Feature that flags up accounts that have searched for or accessed websites that might be linked into cyberbullying or self harm.

The Network Manager E safety responsibilities include:-

- To provide technical support and perspective to the DSL and Senior Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures
- Reporting of any E safety infringements to AHT
- Ensuring all digital communication devices use official school systems
- Ensuring filtering systems are applied and regularly updated
- Keeping up to date with E safety technical information
- Keeping a record of all communication devices within school.
- To ensure that the IT systems are secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- To ensure that appropriate access and technical support is given to the DSL (and/or HT) to our filtering and monitoring systems, to enable him/her to take appropriate safeguarding action if/when required.

Management of applications (apps) used to record student progress

- The Headteacher is ultimately responsible for the security of any data or images held of students.
- Apps/systems which store personal data will be risk assessed prior to use by the network manager.

- Personal staff mobile phones or devices, including cameras will not be used for any purpose which records and stores student's personal details, attainment or photographs.
- Only School issued devices and cameras will be used for the purpose of recording and storing children's personal details, attainment or photographs.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.

Safety and Responsibilities for Staff

All staff are required to read and sign an Acceptable User Policy (AUP) which clearly states the responsibilities of staff using technology in the workplace. This will be signed when they commence their employment at Presfield and will be reinforced each year during the staff's E-Safety Session. The AUP lists the responsibilities of all staff and covers the use of digital technologies in school: i.e. E-mail, Internet, Intranet and network resources, Learning Platform, software, equipment and systems and complements the General Teaching Council's Code of Practice for Registered Teachers. (See appendix 1)

E-Safety training will be provided to all members of staff once a year and it is each person's responsibility to attend this session. Online E safety courses may be required to be completed to keep up to date with current practice.

It is very important that staff make sure that students they are responsible for are using the Internet safely. All Presfield students can be described as "high risk".

Staff responsibilities include:

- To have an awareness of online safety issues, and how they relate to the students in their care. To model good practice in using new and emerging technologies and demonstrate an emphasis on positive learning opportunities rather than focusing on negatives.
- To embed online safety education in curriculum delivery wherever possible.
- To identify individuals of concern, and take appropriate action by working with the DSL.
- To know when and how to escalate online safety issues, internally and externally.
- To be able to signpost to appropriate support available for online safety issues, internally and externally.
- To maintain a professional level of conduct in their personal use of technology, both on and off site.
- To take personal responsibility for professional development in this area.

E-Mail

i. School

Email is widely used within Presfield and is a commonly used form of communication for school business including weekly and daily notices. Staff are expected to check their email regularly when in school. Staff are not expected to access emails outside of work hours. Some staff members may choose to send emails outside of work

hours as it suits their personal life but this is not an expectation. Staff are advised to not have alerts on their own phones. Presfield High School is committed to supporting a home work life balance.

- Staff should be aware that emails have equivalent status in law to letters and faxes and can be disclosed in court.
- Staff must ensure that their use of email is lawful and does not compromise the school's MIS system or damage the school or its employee's reputations.
- Staff are not to send externally any staff/student information without consent of the head.
- Staff must comply with relevant licence terms and conditions when copying or downloading material from or via email.
- Any electronic communication which contains any content which could be subject to data protection legislation (GDPR) must only be sent using secure and/or encrypted methods.
- Staff must be aware to take particular attention when sending any emails that contain potentially sensitive or confidential information as school emails are not encrypted.
- School Emails should not be used for commercial purposes.
- Emails may be monitored for the purpose of ensuring appropriate use.
- Staff should use a secure email system such as 'egress' when sharing sensitive information with other agencies whenever possible.

ii. Personal

- Personal emails should only be accessed outside teaching/working hours. No communication with students or parents should be conducted through personal email. All communication should be through school email. Access in school to external personal email accounts may be blocked

iii. Inappropriate email use

Email should not be used to abuse or inflame others or to harass or threaten. Responding to abuse will not be accepted as an excuse for using abusive language.
Emails must not be sent that contain obscene, abusive or profane language. If staff members receive abusive or threatening e- mails they should inform the head.

Social media/networking

Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- Many staff use social networking sites such as Facebook and Twitter. Access to such sites should only occur outside of lessons. No staff member should be accessing social media in the presence of students.
- Staff should not communicate with students or parents via social media. All communication should be via letter, phone or email. Any friendship requests made by current students and parents should be declined. Friendship requests from ex students under the age of 24 should also be declined. Contact can be conducted via school email. All social media devices should have privacy settings which do not allow students or parents to access staff personal conversations. Geo-location settings should not be available for students or parents to access.

Staff should ensure they “log out” of any social media sites to ensure access is prevented by third parties.

- Staff should be aware that any posts/comments on social media are potentially available to the wider public and consequently should reflect your professional status. Comments can be taken out of context so staff must remain vigilant about any comments made or language used.
- Staff must not engage in any role/school related discussion online (outside of formal channels). Discussions about their employer, colleagues, pupils or their families are strictly forbidden.
- Posting content that could be considered defamatory, derogatory or in breach of copyright legislation which could bring the school into disrepute will result in disciplinary action following the schools agreed disciplinary code.
- Staff must not share personal or confidential information about the school, its staff or pupils online. Examples of this kind of information are staff changes, terms of employment, procurement, business partnerships and personal information about colleagues and children. Information of this kind must never be shared on social media. Where there is a legitimate reason to share information the school business processes must be followed.
- Staff should not publish personal information such as their age, home address or any other information you would not want pupils to know.
- If staff are unhappy about any content they should follow the reporting misuse protocol
- Official use of social media sites as communication tools will be risk assessed and formally approved by the network manager
- The school has a facebook page and the school therapy dog has an instagram page. Both of these are monitored by multiple members of SLT including the Head and Deputy head who have passwords for the accounts.

Internet

Staff must ensure that their internet use is lawful and does not compromise the school's MIS system or damage the school or its employee’s reputations. Staff must comply with relevant licence terms and conditions when copying or downloading material from the internet.

- School internet should not be used for commercial purposes.
- Personal use must only be accessed outside of teaching/working hours.
- Users must not commit the school in any way to purchasing or acquiring goods and services without approval from a member of the SLT

Internet usage may be monitored for the purpose of ensuring appropriate use.
Staff must not send, access, display, download, copy or circulate any inappropriate stories, jokes or anecdotes, which are of the following nature

- Pornography or sexually orientated images
- Gambling
- Gaming
- Discrimination
- Racial or religious hatred
- Promotion of violence
- Illegal or unlawful acts

If inappropriate material is accessed accidentally, school employees should immediately report this to the Deputy Head or Head teacher so it can be taken into account as part of any monitoring procedure.

The school reserves the right to take disciplinary action if any staff member fails to comply with this direction. Any disciplinary action will be in accordance with the school's disciplinary procedure.

Personal Devices and Mobile Phones

Electronic devices of all kinds that are brought into School are the responsibility of the user at all times. Presfield School accepts no responsibility for the loss, theft or damage of such items. Nor will the School accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- Mobile phones and personal devices are not permitted to be used in classroom areas within the School site.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Presfield School community and any breaches will be dealt with as part of the School discipline/behaviour policy.
- Members of staff will be issued with a School/work phone number and email address where contact with students or parents/carers is required.
- All members of the School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene School's policies.
- School mobile phones and devices must always be used in accordance with the AUP

Data Protection

Data will be recorded, processed, transferred and made available according to GDPR / 2018

GDPR / Data Protection Explained -

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Staff must ensure that they:
• At all times take care to ensure the safekeeping 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

Use of digital and video images – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students 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 reduce the likelihood of the potential for harm:

• When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
• Staff are allowed to take digital / video images to support educational aims, but must follow school protocol concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
• Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Students must not take, use, share, publish or distribute images of others without their permission
• Photographs published on the website, or elsewhere that include students / students are carefully selected and comply with good practice guidance on the use of such images.
• Written permission from parents or carers will be obtained before photographs of students are published on the school website. (see appendix)

Only students first names will be used anywhere on a website, facebook, twitter or blog, particularly in association with photographs

Recording of school events

Parents and carers may take photographs and recordings of school events solely for their own personal use and not for publication on the internet or elsewhere. Use of

images for such purposes would require permission of all parents/carers of students involved.

Preventing Radicalisation

Preventing Radicalisation is part of our commitment to keeping children safe online. Radicalisation refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. In March 2015, statutory duties were placed on schools by the Counter Terrorism and Security Act (2015) which means we must work to prevent children being drawn into extremism. We do this through continual vigilance and monitoring of student ICT use. Staff have completed Home office Prevent training online and have also had prevent training from Merseyside police.

Statutory Duties

The duty to prevent children and young people being radicalised is set out in the following documents.

· Counter Terrorism and Security Act (2015)
· Keeping Children Safe in Education (2023)
· Prevent Duty Guidance (2023)
· Working Together to Safeguard Children (2018)

The Department for Education has dedicated a telephone helpline (020 7340 7264) to enable concerns relating to extremism to be raised. Concerns can also be raised by email to counter.extremism@education.gsi.gov.uk .

Please note that the helpline is not intended for use in emergency situations, such as a child being at immediate risk of harm or a security incident, in which case the normal emergency procedures should be followed.

Safety and responsibility for Students

All students will receive E-Safety training at the beginning of each year as part of their ICT lesson. Students who are absent will revisit the work to ensure full coverage. All students will then sign an AUP (see appendix 2) during these specific E Safety ICT lessons.

This document will clearly state their responsibilities when using technology in school. All students will be taught how to use all technologies in a responsible and safe way. This will be part of the ICT and life skills curriculum.

Student mobile devices including phones are prohibited for pupils during the school day. Any such devices must be handed into form staff on arrival and will be returned at the end of the day to allow usage when travelling. Special consideration can occur where the device supports sensory needs or self-regulation.

Any use of mobile phones must be within the AUP guidelines. In exceptional circumstances where the student’s EHCP suggests they should have access to their mobile phone, the headteacher, deputy headteacher or assistant headteacher can authorise this.

If a student violates the policy, the phone or device will be confiscated and will be held in a secure place.

- Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting). Staff will not view images of students which are of a sexual nature. If a student's mobile phone is confiscated it will be by a member of the SLT of the same sex of the student as a precaution in case an image is accidentally seen.
- Searches of mobile phone or personal devices will only be carried out in accordance with.
- www.gov.uk/government/publications/searching-screening-andconfiscation)
- Students' mobile phones or devices may be searched by a member of the Senior Leadership Group, with the consent of the student or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. www.gov.uk/government/publications/searching-screening-and-confiscation)
- Mobile phones and devices that have been confiscated will be released to parents or carers.
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation and both the student and the parent will be informed of this.

No student may appear on the Web Site or in promotional material without their parent/carers consent, the consent form is completed when the student starts school and is kept on record until they leave; it will only need amending if the parent/carer would like to change it.

E-mail

Students may only use approved email accounts on the school system. Students must immediately tell a teacher if they receive an offensive email. In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. Incoming e-mail should be treated as suspicious and attachments will not be permitted in pupil accounts. The forwarding of chain letters is not permitted

Cyber bullying

Presfield school is committed to addressing any incidents of bullying including cyber bully which can occur at any time during the day through a wide variety of "platforms" including:-

- text messaging
- Picture or video clips
- Phone calls
- Emails
- Online chat rooms

- Instant messaging

- Websites
- Online multiplayer games

Staff will remain vigilant and aware of potential forms cyber bullying might take. These include:-

- Filming-on line fights using electronic messages
- Harassment-Repeatedly sending offensive messages
- Denigration-sending or posting material about a person to damage his or her reputation or friendships
- Impersonation-posing as a person and posting material to make a person look bad, get into trouble or danger, or to damage a person's reputation or friendships
- Outing and trickery-sharing someone's secrets or embarrassing information or images on line or tricking someone into revealing such information and then sharing
- Exclusion-Intentionally excluding someone from an online group
- Cyberstalking-repeatedly sending threatening and intimidating messages or engaging in other online activities that make a person afraid for their safety.

Students are taught measures to help prevent Cyber bullying. These include:-

- Talking to staff if they feel uncomfortable or bullied by a message received
- Ensuring all sent messages are suitable to be read by a responsible adult
- Awareness that serious incidents of bullying will be reported to the police
- Save all messages of a dubious nature to allow investigation
- Record the time and date any inappropriate messages were sent
- Do Not reply to or forward any bullying messages
- Do Not give out personal information on-line including passwords

Social networking

Students are not allowed onto social networking sites during the school day.
Students are not to send friendship requests to staff via social media as these will be declined. In the case of the school facebook page students can send friendship requests. If they attempt to send private messages they will not receive a reply but will be spoken to in school. As stated, multiple members of SLT monitor these accounts.

- Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, School attended, Instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs etc.

- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

- Students will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use as part of life skills teaching with students.

Mobile devices/game consoles

Students will use mobile devices and game consoles during their transport to school. Upon arriving at Presfield all such devices should be handed into form tutor staff and will be returned at the end of the day. If a student has identified sensory needs they may be permitted to use a device for self -regulation purposes.

AI & Chat GPT

AI has recently made great advancements when it comes to using existing content to generate it within a new form. AI systems such as ChatGPT are freely available online and some are even built into web browsers such as Bing. They allow to to do various things such as:

- Generate text based on given input e.g. write me a 2,000 word assignment on e-safety
- Create imagery from prompts
- Replicate sounds including that of peoples voices
- Produce videos including deep fakes which mask someone else's face over another person.

Due to this, students should not use AI such as ChatGPT for malicious reasons such as plagiarising work, producing inappropriate images, replicating the sound of other students/staff members voices or attempt to create a deepfake.

Consequences

Any student who is found to have behaved in an inappropriate way in terms of E safety will face consequences as per the school behaviour policy. Issues of bullying and E safety will be recorded, monitored and presented to governors through the AH behaviour update report. Issues of a serious nature will be reported to the police. Parents will be informed of any e safety infringements and subsequent consequences.

Student misuse/inadvertent misuse

If a student accesses or has inappropriate material/communication sent to him/her they should inform the teacher immediately. The teacher should switch off the screen to the computer but leave the computer logged on. The network manager should be informed as a matter of urgency. The Head teacher or in the Head's absence the

Deputy should be informed. They will decide if the matter requires referral to DSL. The network manager can then access the student's computer and follow the trail to ascertain if any internet filter breaches have occurred.

The network manager can then block the offending website. Staff, after consulting the technician, will decide upon any action required. Parents will be informed of the incident regardless if action is required.

Support for Parents

As a school we believe it is our duty to support parents and carers in keeping their child safe while using technology within the home environment. Computers and other devices in the home are more open and don't have the security features which we have in school, which does make the child more vulnerable in this environment.

The parents will be invited to E-Safety sessions which will be held in school at the beginning of the school year. Two sessions will be offered one during the school day and the other after school. E safety talks will also take place in the year during coffee mornings to support parents.

The school website will have information regarding E-Safety for parents / carers and young people.

Sometimes a parent may raise concerns about the progress of their child, behaviour concerns etc. via a Facebook wall or online message board. In all cases, the appropriate communication processes publicised by the schools should be used. These processes have been designed to support professional and confidential discussion and problem resolution.

Where parents and carers are invited to comment on children's online work, guidance should be provided to ensure all comments are positive and supportive. It is not acceptable for anyone to post negative comments about any child on social media and the school needs to be careful to ensure they are not complicit in this occurring.

Final Note

All school stakeholders are expected to model appropriate online behaviour and good judgement in content published online. The school may be monitoring social media and will take seriously any content that could have a negative implication for the school, its staff, the pupils or the community it serves.

Staff Acceptable Use Agreement 2023

As a member of Staff at Presfield High School you have a clear professional responsibility for children's safeguarding. It is important that you recognise and understand the necessary measures that must be taken to protect data and information systems from infection, unauthorised access, damage, loss, abuse or theft. All staff members must act in a lawful and ethical way.

Please read and sign this Acceptable Use Policy

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal or share my network or Google password(s) to anyone.
- I will not log on for another person
- I will not allow unauthorised individuals to access E-Mail / Internet / Intranet / network, or other school / LA systems.
- I understand that there is a difference between my professional and private roles. I will not engage in any online activity that may compromise my professional responsibilities, this refers to social network sites such as Facebook and Twitter.
- I will only use the approved, secure EMail system(s) for any school business.
- I will only use the approved school EMail, school Learning Platform or other school approved communication systems with students or parents/carers, and only communicate with them on appropriate school business.
- At any time I will not use school equipment to browse, download or send material that could be considered offensive or inappropriate to colleagues or students.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Head teacher.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other devices (including USB flash drive), to the network / Internet or computer that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not connect a computer, laptop or other devices, to the schools network / Internet or a computer without first taking advice from the schools Network Manager
- I will not use personally owned digital cameras or camera phones for taking and transferring images of students or staff without permission and will not store images at home.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role and will not be used to bring the school into disrepute.
- I agree and accept that any computer, laptop or IPad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school if a reasonable amount of personal use outside of school hours becomes "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's E-Safety curriculum into my teaching/support.
- I understand that all Internet usage / and network usage is monitored and that monitoring data could be made available to any member of the SLT.
- I understand that failure to comply with this agreement could lead to disciplinary action.

I have read and understood and agree to comply with the Staff Acceptable Use Policy

Signed: ..... Print Name: .....

Date: .....

Student acceptable use agreement 2023

Policy for using school computer services.

- be aware that your treatment of school computer services is supervised and your screen can be captured at any point, so only use them for your studies
- do not eat or drink in computer areas
- leave areas tidy when you leave
- do not change any of the system settings
- report any faults to a member of staff
- do not install any software
- do not make copies of any software
- do not try to open any materials that are not linked to your studies
- do not make malicious use of AI such as ChatGPT

If students need to use a memory stick they must be scanned by the network manager before being used on the Network.

Policy for using the Internet in school.

Only use the Internet to search for materials that are linked to your studies or when given permission by a member of staff, for areas of personal interest which is appropriate for school.

The Internet must not be used for:

- Downloading illegal, offensive or obscene material.
- Creating websites that are obscene, defamatory, or infringe copyright.
- Creating commercial websites.
- Opening any email service or chat rooms except school email.
- Downloading program files, including gaming software or media files (unless this is part of your studies and your tutor has given consent).
- The downloading of any form of 'virus' software.
- You must not send any offensive messages by school email
- If you send attachments to an email it must be under 25Mb in size.

The school is not responsible for what you send in emails, and can pass on your details to a suitable authority if anyone complains about an email you have sent.

Policy for using the school's network systems

If your storage becomes full, you can ask a member of staff if it can be increased
Do not share your password with anyone
Do not log on to anyone else's account, access their files/emails, or destroy, copy alter or move anyone else's files.
Only access your own folder on the network
Do not change any access rights to folders on computers or network areas.
Only use the device that has been given to you by a member of staff.

Agreeing to this policy

It is important that you understand your responsibilities, so if you are ever unsure about what is allowed, always ask a member of staff.

Abusing the school's computer services can result in disciplinary action and the passing on of your details to a suitable authority.

The school may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it is believed that unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the school suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Computer Acceptable Use Policy.

Student Signature: ..... Print Name: .....

Parent Signature: ..... Date: .....

Parental consent for use of digital images 2023

Dear Parents/Carers,

As part of our communication link with parents we will be using social media platforms such as Facebook and Twitter.

As you are aware we have to be extremely careful with the internet so no pictures will be posted without your permission.

Please complete the slip below regarding permission for the use of your child's image. A pupil's name will never be printed with the image.

If you have any concerns or queries about our social media sites, please do not hesitate to contact me.

Yours sincerely,

Lucy McLoughlin
Headteacher

I give permission for ..... picture to be used

☐ on the school website ☐ on school social media (Facebook, Twitter etc.)
☐ on private Facebook group
☐ on marketing material - prospectus, news articles etc.

Signed..... Date.....

Reporting Misuse Protocol

All incidents of Misuse should be reported to the Head Teacher and the following protocol observed.