E-safety Policy

Responsibility	Fiona Lovecy
Date of last review	June 2025
Date of next review	June 2026
Approved by	PHS Governors
Approval date	
Version Control	V1 Original

This 'E-safety Policy' operates in conjunction with other policies-e.g. 'Behaviour Policy', relevant school's 'Behaviour for Learning Protocols', 'Mobile phone contract' and 'Safeguarding Policy'.

1. Aim

We recognise the value of modern technology systems and welcome their development. We continually strive to enhance their appropriate use (both within our schools and outside) in order to promote the educational attainment of our students. This policy is of paramount importance as our students' access to technology is currently becoming universal and increasingly more mobile. We aim to ensure we have an effective approach to online safety, which enables use to protect and educated the whole school community in its use of technology.

The technologies encompassed by this policy include all computer and internet technologies and electronic communication devices such as mobile phones, tablets etc

We aim to have robust processes in place to ensure the online safety of students, staff, volunteers and governors.

The four key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, disinformation, misinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism. Common risks we address with students within content focus on exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse. We also focus on lifestyle websites, for example pro-anorexia/ self-harm/ suicide sites, and so-called "hate sites". Equally, we believe that it is important that students are taught to check the authenticity and accuracy of any online content they look at.
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes. Dangers we address with students here include grooming, all forms of cyber-bullying, as well as identity theft (including so-called "frape", the hacking of Facebook profiles) and password security.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and seminudes and/or pornography), sharing other explicit images and online bullying; Within this area, students are taught about privacy issues, including disclosure of personal information, as well as digital footprint and online reputation. They are also taught about the need to consider health and well-being, where necessary limiting the amount of time spent online (internet or gaming). Equally, we believe it is important that students are educated about the dangers of sending or receiving personally intimate images, and of infringing music and film copyright laws.

and

- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyberbullying: advice for Headteachers and school staff

- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL). They will ensure all staff undergo online safety training and ensure all staff understand their roles and responsibilities around filtering and monitoring. The governor who oversees online safety is Mrs Sandy Poulton (Safeguarding Governor).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures and is included in the curriculum to cover all aspects of how students should keep themselves and others safe online.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and Deputies are set out in our Safeguarding Children Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school and is reviewed as required
- Working with the Headteacher, Network Manager, Data Protection Officer and other staff, as necessary, to address any online safety issues or incidents
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and networks and reporting to back to Governors on this process and the effectiveness and responses
- Working with the ICT manager and online safety team to make sure appropriate systems and processes are in place and address any concerns and incidents.
- Managing all online safety issues and incidents in line with the school child protection policy alongside Heads of House/6th Form Lead
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy- alongside Heads of House and the Assistant Head (Pastoral)
- Updating and delivering staff training on online safety

- Liaising with other agencies and/or external services if necessary
- Providing reports on online safety in school to the Headteacher and/or governing body

This list is not intended to be exhaustive.

3.4 The Network Manager

The Network Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems daily
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.5 All Staff and long term volunteers

All staff are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that students follow the school's terms on acceptable use (Appendix B)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures by speaking to the DSL and then then IT tech team if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school's Student Conduct (behaviour) Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here.'

This list is not intended to be exhaustive.

3.6 Parents/Carers Parents/Carers are expected to:

- Notify a member of staff or the DSL of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix A)

Parents/Carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware key policy points, when relevant, and expected to read the ICT use leaflet. If appropriate, they will be expected to agree to the terms on acceptable use.

Internet usage

The internet is used within the schools to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the schools' management information and administration systems.

We recognise the importance of the internet as an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for students who show a responsible and mature approach to its use.

Students will use the internet outside of schools and part of our responsibility is to educate them in safe use of the technology.

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study. It is also taken from the guidance on relationships education, Personal, Social, Health and Relationships Education (PSHRE). All schools have to teach: Relationships and sex education and health education in secondary schools.

In Key Stage 3, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Safe internet use including methods of hacking used to trick people, password security, social engineering, the risks of removable storage devices such as USBs, multi-factor authentication, how to report a cyber incident or attack and how to report an personal data breach.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- The risks of online radicalisation
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

5. Educating Parents/Carers about Online Safety

The school will raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers via the website.

The school will let parents/carers know:
- What systems the school uses to filter and monitor online use
- Types of tasks students are being asked to do online, including the main sites they will be asked to access.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Head of House**.**

Use of the internet within the school

Amongst the uses of the internet within our school are the following:

- Access to learning wherever and whenever convenient.
- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with the Local Authority and DfE.

6. Cyberbullying

6.1 Definition

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Student Behaviour Policy.)

6.2 Preventing and Addressing Cyberbullying

To help prevent cyberbullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyberbullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyberbullying with their tutor groups. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes Personal, Social, Health and Relationships (PSHRE) education, and other subjects where appropriate. All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support students, as part of safeguarding training. The school also provides information on cyberbullying to parents/carers via the school website so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyberbullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained. Staff will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Head of School, DSL or senior member of staff.

- Explain to the student why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the student's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, a suitable response will be decided upon. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if or request parents delete them if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- School behaviour policy and searches and confiscation school guidance

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Pershore High School recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Pershore High School will treat any use of AI to bully students very seriously, in line with school policies.

Staff should be aware of the risks of using AI tools while they are still being developed and should assess any risk when new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, students and staff.

7. Acceptable Use of the Internet in School

All students, parents/carers, staff, volunteers and governors are expected to read and adhere to an agreement regarding the acceptable use of the school's ICT systems and the internet. (Appendix A for Students AUP). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet

must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in the appendices of this policy (students, parents/carers) and the ICT User Policy (staff, volunteers and governors).

Publishing students' images and work

- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students' full names will only be used when featured on news articles sent to press.
- No photographs of students are published on the schools' website without permission from the parent/carer. Student work can only be published with the permission of the student.

8. Students Using Mobile Devices in School

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device. Students will be advised of appropriate mobile phone use in school.

Students in Years 7-11
Mobile phones/electronic devices can be a distraction to the learning process and are not required during school time. Any mobile phone/electronic device in plain sight will be confiscated and taken to the student hub. Repeat offences will only returned to the appropriate parent/carer who will need to collect it from the school office. Any mobile phone or other device that is brought into school is entirely at the risk of the student. The school will not be responsible for any loss or damage to the device. In the event of an emergency the school office is happy to pass urgent messages on to students so that the use of a mobile is NEVER necessary within school.

Sixth Form
Students in Years 12 and 13 are permitted to use mobile phones in the Sixth Form Centre only. In setting an example to students in the Lower School, personal devices must not be used in other parts of the school.

All Students
The filming or recording by mobile phones in school is prohibited and if the school is made aware that such activity has occurred and shared, e.g. via social media the school reserves the right to impose sanctions which may vary depending on the severity of the offence, including suspension or permanent exclusion even for a first offence.

Exceptions where specific permission is granted by the teacher
- Mobile phones or similar devices and headphones/ear pods have a valid use for some ICT, iMedia and Music courses as they enable students to store documents and therefore take work home with them. These devices should not be seen or used at any time other than in lessons where permission has been given. Any mobile phone or other device that is brought into school is entirely at the risk of the student. The school will not be responsible for any loss or damage to the device.
- It may be appropriate for headphones to be used with computers eg Language work, but under no circumstances should they be used simply to listen to music.

9. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Any student in breach of the agreement for usage of the Internet may have their access curtailed immediately pending an investigation.
Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Disciplinary Procedures/Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Social Networking services
Access to Social Networking services (for example Twitter, YouTube, Facebook, Instagram, Snapchat, Pinterest and TikTok) is forbidden in our school by students and all such sites are blocked. Students using such sites outside of our school have a duty to use them responsibly. Any incident of slander, abuse or defamation perpetrated on a

social networking site which impacts upon one of our students, shall be treated as bullying and shall be sanctioned in accordance with the School's behaviour policy.

10. Monitoring arrangements

The DSL and staff log behaviour and safeguarding issues related to online safety. The school internet facility has been designed expressly for student use and includes filtering (Smoothwall) appropriate to the age of students. Appropriate use is monitored through the Senso monitoring system which records key word searches/use and images. All students must read and accept the 'Student IT Acceptable use policy' before using any of our IT resources. The DSL keeps an incident log recording online breaches and actions. Safeguarding concerns are recorded on CPOMS. This policy will be reviewed every year by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing body.

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can accept no liability for the material accessed, or any consequences of Internet access.

11. Links with other policies

This online safety policy is linked to our:

- Safeguarding Children Policy
- Child-on-Child Abuse Policy
- Student Behaviour Policy
- Staff Code of Conduct
- Staff Disciplinary Procedure
- Acceptable User Agreements
- Data Protection Policy and Privacy Notices
- Complaints procedure
- School mobile policy

12. Staff Training

Staff will receive annual training on E-Safety as well as updates in briefing and in Safeguarding briefing sheets. All staff are required to complete Cyber Security Training.

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

.

Appendix A

ICT ACCEPTABLE USE POLICY FOR STUDENTS

This policy applies to all students of the school who are provided with access to the school's ICT network. Pershore High School fully recognises its responsibilities for safeguarding children. Safeguarding in this case also applies to the acceptable use of ICT equipment in order that the school is not compromised in any way as a result of inappropriate materials being accessed or downloaded.

Before using school ICT equipment all users must accept the terms of this policy, acceptance of the policy will be recorded each time the user logs on to the network.

- I will only use the school's email, Internet and network for legitimate purposes. Forwarding chain letters by email is not permitted.
- I will keep my network password secure and will not allow others to use them to gain access to school resources.
- I will not attempt to gain access to other users' user areas or non-public locations on the school network.
- I will not browse, download, or send material that could be considered offensive. Material that victimises, harasses, or bullies others is strictly forbidden.
- I will not publish or give away personal information that could identify me or other students or staff.
- I will not arrange to meet anyone met through the internet or via email.
- I will not access social networking sites on school ICT equipment.
- I will not use social media negatively to cause offence, upset or bully any staff or students.
- I will report any accidental access to, or receipt of, inappropriate materials as well as inappropriate websites accessible via the school internet connection to the school's e-Safety Officer (Mrs Lovecy).
- I will not attempt to load or download any software or resources that can compromise the network or are not adequately licensed.
- I will not connect personal laptops or other hardware to the school network or Internet without permission from the school's ICT Support Team.
- I will not use any device to record or transfer images, video content or audio recording of myself or others without permission.
- I will not use my mobile phone during lessons or school activities unless given permission by a member of staff.
- I understand that my use of school ICT equipment will be monitored and that all ICT use that contravenes the Acceptable Use Policy will be logged, sanctions will be issued and in serious cases a computer ban enforced.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action and that evidence of it may breach the Computer Misuse Act 1990 and may be passed to the Police.
- I will recognise the risks of AI including accessing harmful content or being bullied and avoid using AI inappropriately for school work. I will follow and respect school guidelines in positive use of AI tools.

Sixth Form Only:

Sixth Form students have access to the school's Wi-Fi network PHS Sixth Form and can login using their normal school username and password.

Signed……

Name (printed)……

Date……

Appendix B

ICT ACCEPTABLE USE POLICY FOR STAFF

Pershore High School fully recognises its responsibilities for safeguarding children. This policy is to be read in conjunction with the Safeguarding Children Policy.

This policy applies to all adults employed by the school who are provided with access to the school's ICT network. Pershore High School fully recognises its responsibilities for safeguarding children. Safeguarding in this case also applies to the acceptable use of ICT equipment in order that the school is not compromised in any way as a result of inappropriate materials being accessed or downloaded.

Before using school ICT equipment all users must accept the terms of this policy, staff will be required to sign an agreement form.

- I will only use the school's email, Internet and network for professional purposes or for uses deemed 'reasonable' by the Head Teacher and Governing Body.
- I will keep my network, SIMS, CPOMS and other passwords secure and will not allow students to use them to gain access to these resources.
- I will use the approved, secure email system for any school business. See below for use of other social media.
- I will not deliberately browse, download or send material that a reasonable person would find offensive.
- I will report any accidental access to inappropriate materials to the school's e-Safety Officer (Fiona Lovecy)
- I will not load or download any software or resources that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other hardware to the school network or Internet that do not have up-to-date versions of anti-virus software.
- I will not use any digital device to transfer images of students or colleagues without permission.
- I will not use any external drive to store work related files and those containing personal data
- I will delete files containing personal data e.g. exam results are destroyed 5 years after the student turns 18 or sooner where there is no lawful reason to store this data for longer
- I will not include current students as my friends in my personal social networking sites such as Facebook.
- Use of Social Media – staff who wish to communicate with students using social media may only do so for educational purposes. Staff must follow these guidelines:
  - The site must be registered to the school and should include PHS or Pershore High School in the title.
  - The Leadership Team (PH) will hold a register of sites and staff must register them before use with students and keep the details up to date.
  - The register must include the username and password of the administrator of the site and this must be updated should changes occur.
- A school user should, where possible, be included for monitoring/safeguarding purposes: monitor@pershore.worcs.sch.uk.
- I will ensure I am aware of the school e-safety policy so that it is appropriately embedded in my classroom practice.
- I will not allow unauthorised individuals to access the school network, email or Internet connection.
- I understand that my use of school ICT equipment will be monitored and that all ICT use that contravenes the AUP will be logged.
- I will ensure that when my laptop is left unattended it is locked with a password to prevent unauthorised access to potentially sensitive materials.
- I will avoid displaying student personal details in such a way that they could be viewed by other students (e.g. projecting my laptop screen in a classroom).
- This policy is to be read in conjunction with the Code of Conduct and Safeguarding policy.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action and that evidence of it may breach the Computer Misuse Act 1990 and may be passed to the Police on request.

Signed ……..

Print Name……Date……..

Appendix C

Remote learning policy

1. Aims

Where a student, class, group or small number of students need to self-isolate, or there is a local lockdown requiring students to remain at home, DfE expects schools to be able to immediately offer them access to remote education. Schools should ensure remote education, where needed, is high-quality and aligns as closely as possible with in-school provision.

This remote learning policy for staff aims to:

- Ensure consistency in the approach to remote learning for students who are not in school for COVID related reasons
- Set out expectations for all members of the school community with regards to remote learning
- Provide appropriate guidelines for data protection

2. Roles and responsibilities

2.1 Teachers

When providing remote learning, teachers should, wherever possible, be available between 8:30 am and 4:00 pm.

If they're unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the normal absence procedure repeated here:
*In the event of unplanned, emergency absence **all staff** must email absence@pershore.worcs.sch.uk by 7.30am on the first day of absence, please ensure that your line manager is also copied in on the email – If for any reason this is not possible then a message can be left on the voicemail (01386 552471 ext. 232) with a follow up email sent as soon as you are able. Teaching Staff - If your absence is to continue for more than one day, please contact absence@pershore.worcs.sch.uk before the end of the first school day, thus giving time to arrange a supply teacher.*

Remote learning will be provided in different forms depending on need:

- Short term absence for small numbers of students (e.g. individuals and part-classes self-isolating) – Teachers will try, as far as possible, to match remote resources to the curriculum delivered in school – this could take the form of resources prepared by the teacher/department for normal in-school lessons, use of external resources from GCSEPod, BBC Bitesize and Oak Academy.
- Absence of whole cohorts of students (e.g. a year group self-isolating due to a positive case or Tier 2 Rota requirements). Teachers will provide resources as above in addition to Teams Lessons for as many normally timetabled lessons as possible but as a minimum for 50% of the timetabled periods.

When providing remote learning, teachers are responsible for:

- Setting work:
    - Provide work for students unable to attend school to closely match as far as possible the work covered in lessons for students' peers in school or the planned scheme of learning. In the event of a colleague being unwell to set work for that teacher's classes as requested by the Head of Department
    - Provide work commensurate with what would be required during in–school lessons as far as possible
    - As far as possible make this work available by 6pm on the day before it is required
    - Work must be accessible via Microsoft Teams and Class Notebook following training at the staff meeting on 12/10/20. Notifications regarding the work should also be available via ePraise with a link, where possible to the resources.
    - Where possible work should be set at departmental level to reduce the burden on individual teachers – however this is not the responsibility of the HoD and should be shared between all subject teachers to reduce workload.

- Providing feedback on work:
    - Teachers should request that work requiring feedback/marking should be returned using Class Notebook
    - Teachers should use Class Notebook to provide students with appropriate feedback in line, as far as possible, with the departmental marking policy
    - Teachers will use their discretion regarding assessing work that is returned after any clearly shared deadline

- Keeping in touch with students who are not in school and their parents:
    - Day to day welfare calls will, where possible, be undertaken by staff in the Student Hub. Should numbers of students self-isolating increase, Tutors may be required to make welfare calls using the 3CX phone system
    - Teachers/Tutors are not expected to respond to emails/phone calls outside of their normal working hours outlined above 8:30am to 4:00 pm
    - Complaints regarding online provision should be directed to the relevant Head of Department/Head of House
    - Concerns regarding the behaviour of students during remote learning should be directed to the relevant Head of Department/Head of House
    - Safeguarding concerns must be recorded on CPOMS and should a member of staff have an immediate concern the CPOMS entry must be flagged to safeguarding@pershore.worcs.sch.uk or direct to a member of the safeguarding team: ZB, PH, AN, DC, CJB, AC, RK
- Virtual meetings with staff, parents and students e.g. individual meetings, online Parents' Evenings:
    - Staff should be formally dressed during normal working hours (including for Parents' Evenings) and appropriately dressed; smart-causal outside of these times
    - Staff should blur their background or use a digital background to avoid displaying their home environment. If the home environment is not conducive to quality lesson/meeting delivery staff should deliver their sessions from school

2.2 Teaching assistants

When assisting with remote learning, teaching assistants must be available for their normal working hours or between 8:45am and 3:30pm whichever is greatest.

If they are unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the normal absence procedure as above.

When assisting with remote learning, teaching assistants are responsible for:

- Supporting students who are not in school with learning remotely:
    - Those students who require support as directed by the SENCO following, as far as possible, the normal timetable (see above)
    - Provide support through additional Teams sessions where possible, adapting remote learning resources as appropriate and as requested
- Attending virtual meetings with teachers, parents and students:
    - Staff should be formally dressed during normal working hours (including for Parents' Evenings) and appropriately dressed; smart-causal outside of these times
    - Staff should blur their background or use a digital background to avoid displaying their home environment. If the home environment is not conducive to quality lesson/meeting delivery staff should deliver their sessions from school

2.3 Heads of Department

Alongside their teaching responsibilities, subject leads are responsible for:

- Considering whether any aspects of the subject curriculum need to change to accommodate remote learning
- Working with teachers teaching their subject remotely to make sure all work set is appropriate and consistent

- Working with other HoDs and members of the Leadership Team to make sure work set remotely across all subjects is appropriate and consistent, and deadlines are being set appropriately to allow students to meet them
- Monitoring the remote work set by teachers in their subject, monitoring Class Notes, dealing with concerns and through remote meetings with teachers and concerned parents
- Providing details of resources teachers can use to teach their subject remotely and where possible reduce workload

2.4 House Team

Alongside any teaching responsibilities, members of the Pastoral Team are responsible for:

- Supporting the attendance and behaviour of students at remote learning sessions
- Following up concerns regarding student engagement from teaching staff
- Monitoring and dealing with complaints from staff, students and parents
- Following up concerns with the DSL/Leadership Team as appropriate

2.5 Leadership Team

Alongside any teaching responsibilities, senior leaders are responsible for:

- Co-ordinating the remote learning approach across the school
- Monitoring the effectiveness of remote learning through, for example, discussions with HODs and teachers, attending remote learning lessons delivered via Teams, student and parent surveys
- Monitoring the security of remote learning systems, including data protection and safeguarding

2.6 Designated safeguarding lead

The DSL is responsible for:

- Liaising with support and teaching staff, encouraging them to report concerns raised during online sessions or lack of engagement/attendance
- Ensuring that all safeguarding issues are dealt with appropriately
- Contacting and supporting families where serious concerns are raised by staff

2.7 SENCO

The SENCO is responsible for:

- Overseeing support for students with additional needs
- Directing Teaching Assistants to tasks/timetables that support access to remote education for students with SEND

2.8 IT Support staff

IT staff are responsible for:

- Supporting and maintaining Office 365 protocols and remote access systems
- Supporting staff, students and parents with any technical issues they're experiencing
- Reviewing the security of remote learning systems and flagging any data protection breaches to the Data Protection Officer (Karen Bevan)
- Preparing and supporting issues with hardware provided to staff and students for remote learning

2.9 Students and parents

Staff can expect students learning remotely to:

- Be contactable during the school day and attend Teams lessons whenever possible and according to their school timetable
- Complete work to the deadline set by teachers

- Seek help if they need it, from teachers or teaching assistants
- Alert teachers if they're not able to complete work

Staff can expect parents with children learning remotely to:

- Support students to attend remote learning opportunities where possible
- Make the school aware if their child is unwell or otherwise can't complete work
- Seek help from the school if they need it
- Be respectful when making any complaints or concerns known to staff

2.10 Governors

The governors are responsible for:

- Holding leaders at all levels to account in relation to this Remote Learning Policy
- Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible
- Ensuring that staff are certain that remote learning systems are appropriately secure, for both data protection and safeguarding reasons

3. Who to contact

If staff have any questions or concerns about remote learning, they should contact the following individuals:

- Issues in setting work – Head of Department or SENCO
- Issues with behaviour – Head of House
- Issues with IT – IT Support
- Issues with workload or wellbeing – Line Manager
- Concerns about data protection – DPO representative Karen Bevan
- Concerns about safeguarding – DSL, Jenna Butler or Safeguarding Team

4. Data protection

4.1 Accessing personal data

When accessing personal data for remote learning purposes, all staff members will:

- Use their school PC or laptop (with dual factor authentication)
- Have access to SIMS and 4 Matrix and use data according to the school's ICT Acceptable Use Policy

4.2 Processing personal data

Staff members may need to collect and/or share personal data as part of the remote learning system. As long as this processing is necessary for the school's official functions, individuals won't need to give permission for this to happen.

However, staff are reminded to collect and/or share as little personal data as possible online.

4.3 Keeping devices secure

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device – **All files stored in staff user areas are secure on Pershore High School laptops except those stored on the Desktop which are not protected**
- Making sure the device locks if left inactive for a period of time or is manually locked when unattended by the member of staff
- Not sharing the device among family or friends
- Updating antivirus and anti-spyware software automatically (IT Support responsibility)

- Keeping operating systems up to date (IT Support responsibility)

5. Safeguarding

Pershore High School's Safeguarding Policy is updated to reflect remote learning. All staff are required to report any concerns if a safeguarding nature using CPOMS or direct to a member of the safeguarding team – safeguarding@pershore.worcs.sch.uk