CHEPSTOW SCHOOL

INSPIRING LEARNING

CHEPSTOW SCHOOL

E-SAFETY POLICY

Approved by: Full Governing Body

Last Reviewed on: 04.06.26

Next Review Date: June 2027

CHEPSTOW SCHOOL | YSGOL CAS-GWENT

This policy applies to all members of the school community (including staff, students, parents/carers, visitors and members of the community) who have access to school ICT facilities, both inside and outside of school.

Introduction

E-safety focuses on educating students and other members of the school community about both the benefits and risks of using technology, while also providing security measures and empowering users to manage their online experiences. The E-Safety policy at Chepstow School will function in conjunction with other school policies, such as those governing student conduct, bullying, and data protection.

Aims of the policy

The aim of this policy is to protect school community members from harm and provide the information they need to benefit fully from new and developing technology, without endangering themselves or others.

Roles and Responsibilities

This document outlines our school's E-Safety roles and responsibilities of individuals or teams within the school.

Governors

The Digital Safety Policy must be approved by the governors. They are also responsible for evaluating the policy's effectiveness. This will be accomplished by the governing body's subcommittee of the governor regularly receiving information about incidents involving digital safety and monitoring reports. The position of Digital Safety Governor should be assumed by a member of the Governing Body and include:

Regular meetings with the Digital Lead; regular review of the Digital Safety incident logs; regular review of the filtering and change control logs (if practical); and reporting to the appropriate Governors, subcommittee, or meeting

E-SAFETY POLICY

Headteacher

The day-to-day responsibility for digital safety may be passed on to the digital safety lead and child protection lead, however, the headteacher has a duty of care to ensure the safety of members of the school community, including online.

- The processes to be followed in the event of a serious allegation or incident involving digital safety being made against a member of staff or student should be known to the headteacher and (at least) another member of the senior leadership team.
- The Headteacher is in charge of seeing to it that the Digital Safety Lead and other staff members receive the proper training necessary for them to fulfil their roles in digital safety and, as necessary, train other co-workers.
- The headteacher will make sure that a system is in place to enable monitoring and support of those employed by the school who are responsible for internal Digital Safety monitoring.
- The Digital Safety Lead will submit regular monitoring reports to the Senior Leadership Team.

Chepstow School Digital Safety Lead

The digital safety lead takes day to day responsibility for all digital safety issues and has a leading role providing regular incident updates to the school headteacher and ensuring the school policy is reviewed annually. The school's digital safety lead is also responsible for making sure all staff are aware of the procedures in place that need to be followed in the event of an incident taking place, as well as liaising with the school network team on a regular basis.

IT Network

The Shared Resource Service (SRS) / technical staff are responsible for ensuring that the school's technical infrastructure is secure and not open to unauthorised misuse, or malicious attack. The network manager is also responsible for ensuring the network including email accounts, remote access and the internet is regularly monitored in order that any misuse/attempted misuse can be prevented and reported to the Headteacher and Senior Data Protection Officer (School Operations Manager) for investigation.

Teaching and Support Staff

Both teachers and support staff are responsible for ensuring that they have an up to date awareness of digital safety matters and of the school's current policy and practices. All school staff must also

know to report any suspected misuse to the Senior Digital Safety Lead for investigation. School staff must acknowledge their understanding by signing the Staff Acceptable Use Policy.

Teaching and support staff must also ensure that all digital communications with students, parents and carers and others should be to a professional standard and only carried out using official school communication systems.

It is important that all school staff make students aware of any digital safety issues that may arise using aspects of the curriculum and other activities. Monitoring the use of digital technologies in lessons and other school activities and implementing current policies could prevent any issues from arising. When using the internet in lessons, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found.

Designated Safeguarding Person

It is important to emphasise that these are safeguarding issues, not technical issues. The technology provides an additional means for safeguarding issues to arise**.**

The designated Safeguarding person should be knowledgeable in all aspects of digital safety and be aware of the potential for serious safeguarding issues to develop from

- Sharing of personal information
- Access to illegal / inappropriate materials
- Inappropriate online contact with adults / strangers
- Incidents of grooming
- Cyber bullying
- Radicalisation

Students

Students are responsible for using the school digital technology systems in accordance with our Acceptable use policy and are expected to understand the importance of reporting abuse, misuse or access to inappropriate materials and how they report these. Students also need to have a good understanding of the policies in place on the use of mobile devices. They should know and understand the rules in place on the use of images on their mobile devices, and on cyberbullying.

Students should understand the importance of adopting good digital safety practices when using digital technology in and out of school and realise that the school's policy covers their actions out of school, if related to someone with connection to the school.

Parents and Carers

Parents and carers play a crucial role in ensuring that their child understands the need to use the internet and their mobile devices in an appropriate way. As a school, we will take every opportunity to help parents and carers understand these issues through our school platforms. Parents and carers will be encouraged to support the school in promoting good digital safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

CHEPSTOW SCHOOL | YSGOL CAS-GWENT

Policy Statement

Education - young people/students

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

Digital safety should be a focus in all areas of the curriculum and staff should reinforce messages across the curriculum. The curriculum should be broad and relevant. This would include providing digital safety as part of the curriculum within ICT and PSE lessons. Key messages should be reinforced to students during tutorial and pastoral activities and assemblies. It is important that staff act as good role models when using technology themselves to help the students understand the correct and responsible use.

When in lessons that require use of the internet, it is best practice that students are guided to sites that are checked and deemed safe to use, and where students are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites visited.

Education - parents and carers

Parents and carers have a key role in the education of their children and in monitoring their children's online behaviours. Parents may not always be aware of how often children and young people come across potentially harmful and inappropriate materials on the internet and may be unsure of the appropriate way to respond.

Education - staff and volunteers

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

- All new staff will receive access to digital training as part of their induction process.
- The digital safety lead will receive regular updates by attending external training events held by relevant organisations.
- Digital safety policy updates will be presented to and discussed by staff in staff team meetings or on INSET days.

E-SAFETY POLICY

Technical

It is the school responsibility to ensure that the managed service provider (SRS) carries out all relevant digital safety measures. It is also important that the managed service provider is fully aware of the school digital safety policy. The school should also check their local authority on these technical issues if the service is not provided by the authority.

The school will be responsible for ensuring the school network is as safe and secure as possible and that the policies and procedures approved within this policy are implemented. It will also ensure that the relevant persons named in the above sections will be effective in carrying out their responsibilities.

The school technical systems will be managed in accordance to ensure that the school meets recommended technical requirements where required. The network manager is responsible for ensuring the softwares are accurate and that regular checks are made and audits are completed to ensure safety and security of school technical systems.

The acceptable use policy addresses these points in relation to the above sections

- The use of removable media by users on the school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- The provision of temporary access of guests (e.g. supply teachers and visitors) to the school systems.

Bring your own device (BYOD) guidance

There are limited controlled devices linked to our school infrastructure. No other devices should be connected to our school system unless given permission from the network lead.

Use of digital and video images

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

When using digital images, staff should inform and educate students about the risks associated with taking, using and sharing images. Staff have permission to take digital and video images to support educational aims, but must follow school policies. The images should only be taken on school equipment. It is important that images are not distributed of others without requesting permission first.

Photographs published on the school website, or elsewhere that include students will be selected carefully and comply with good practice guidance. Students' full names will not be shared, particularly in association with photographs. Permission will be granted from all parents/carers before photographs are published on the website, or other platforms.

GDPR

See our GDPR policy on school website

Communications

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

The official school email may be regarded as safe and secure. It is monitored regularly. Users should be aware that email communications are monitored and staff and students should therefore only use the email system to communicate with others when in school, or on the school systems.

Users must immediately report to the nominated person any communication that makes them feel uncomfortable, is offensive, threatening or bullying of any nature and must not respond to such communication.

Any digital communication between staff and students / parents and carers must be professional in both content and tone. These communications may only take place on official school systems. Personal email addresses or social media must not be used for these purposes.

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Inappropriate digital activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would be banned from school and all other technical systems. Other activities, such as cyber bullying would be banned and could lead to criminal prosecution. There are however, many activities which may be legal but would be inappropriate in a school setting, either due to the age of the users or the nature of the activities.

As a school we believe that these activities referred to would be inappropriate in our school setting and that users should not engage in these activities inside or outside of school using school equipment.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of digital services. It encourages a safe and secure approach to manage the incident. Incidents may involve illegal or inappropriate activities.

Illegal incidents

If anyone has any suspicion that website(s) concerned may contain inappropriate illegal activities, please report this to the safeguarding lead and Senior Leadership Digital safety lead **immediately**.

Other Incidents

We hope that all members of the school community will be responsible users of digital technology, understanding and following the school policy. However, there may be occasions when breach of the policy could take place, through careless or irresponsible, and very rarely deliberate misuse.

School Action

It is highly likely that schools will need to deal with incidents that involve inappropriate misuse. It is important that any incidents are dealt with as soon as possible in a suitable manner, and that members of the school community are aware that incidents are being, or have already been dealt with.

CHEPSTOW SCHOOL | YSGOL CAS-GWENT

Social Media

As a school we recognise and understand the benefits and opportunities that social media can have. While employees are encouraged to engage through social media, they should be aware that this comes with associated risks, especially around issues of safeguarding and bullying.

Purpose of the policy

Encourage good practice

Protect the school and the employees

Promote the effective use of social media as part of social activities

The policy covers personal and professional use of social media and safe but effective uses

Our policy applies whether social media is being used on school IT facilities, or your own personal devices.

The policy covers all individuals, full time and part time employees, and including those on agency.

Definition of social media

Social media is a broad term for any form of online platform which enables people to interact with each other. It allows people to share all kinds of information.

Examples of social media websites include Facebook, Twitter, Instagram, LinkedIn and YouTube.

Use of social media

All schools and local authorities have a duty of care to provide a safe learning environment for all students and staff.

All staff working at an education establishment are expected to portray a professional approach for students and their families, as well as for other colleagues. Staff should only use a pre-approved school social media account to communicate and share information. These accounts are controlled by the digital lead and/or responsible person within school. The account information is shared with the appropriate colleagues and retained by the school. School staff should not change the account information or password.

Staff should not use the school logo or affiliate themselves on their personal accounts. Any accounts that are identified that are not officially approved, should be reported to the digital lead.

E-SAFETY POLICY

When using school social media accounts the following practices must be observed:

1. School social media accounts must be entirely professional and should reflect well on the school
2. Staff must not publish photos of students without permission from parents/carers. Standard practice is to not publish the student's full name when a photo is included.
3. Staff must consider all safeguarding aspects when creating posts on any social media accounts.
4. Staff must not have 1:1 communication, including direct messaging with students through any social media, apart from school email accounts and online learning platforms.

Acceptable use of social media

Employees should be aware that content uploaded to social media is not private, even if you restrict your privacy settings it is still possible for it to be re-posted or distributed beyond the intended recipients. Therefore, employees should be careful when posting and conduct themselves in a professional manner.

Employees should know of both professional and personal boundaries, and therefore not accept or invite requests from any current or former pupils, or from parents on their personal social media accounts, such as Instagram. All communication with parents via social media should be through the school's social media accounts.

Safeguarding

The use of social media sites can introduce a range of potential risks to children and young people.

Potential risks can include, but are not limited to

- Online bullying
- Grooming, exploitation and stalking
- Exposure to hateful language/behaviour

In order to prevent these risks, the school has the following measures in place to ensure appropriate steps to minimise risk of harm to students and staff.

- Guidance on social media risks and the importance of checking all privacy settings, ensure they are at the highest level possible.

- Clear guidance is provided to ensure staff know what they are expected to report and who they report this too, including taking responsibility and understanding sanctions if procedures aren't followed.
- Detailed risk assessment

Expectations are set by the Education Workforce Council, but all adults working with children and young people must understand the responsibilities that come with working in the setting and their conduct should reflect this.

Roles and responsibilities

School employees should be aware of their online reputation and recognise their online activity can be seen by others, including students, parents and colleagues. Employees should also ensure that any use of social media is carried out in line with this policy and other relevant policies. It is also important that school employees know that any inappropriate use of social media in school may result in disciplinary action, therefore be responsible for their words and actions in an online environment. Staff must consider what they want to post, whether it be a comment, an image or a video and who it could potentially be viewed by. If in doubt of the viewing audience, it is advised not to post.

The school's digital safety lead/leadership within the school are responsible for ensuring that any concerns or questions employees may have on the use of social media are addressed in a timely manner, but within the criteria of the policy ensuring that all staff understand the standards expected of them.

The school's digital lead is responsible for providing knowledgeable advice on the use of social media and reviewing the policy as and when updates are provided.

Policy breaches

Any member of staff suspected to be breaching this policy, this includes complaints received regarding unacceptable use will be investigated. If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with appropriate procedures. Where conduct is considered to be unlawful, the school may report this type of misconduct to the police.

CHEPSTOW SCHOOL | YSGOL CAS-GWENT

Use of Artificial Intelligence (AI)

Purpose

The school recognises the increasing use of Artificial Intelligence (AI) tools (e.g. chatbots, image generators, automated writing tools) and is committed to ensuring their safe, ethical, and appropriate use by pupils, staff, and the wider school community.

Definition

Artificial Intelligence (AI) refers to digital systems and tools that can generate content, respond to prompts, analyse data, or automate tasks in ways that simulate human thinking or creativity.

Acceptable Use

Pupils may:

- Use AI tools to support learning, such as generating ideas, revising concepts, or receiving explanations.
- Use AI under staff supervision where appropriate to enhance creativity, problem-solving, and independent learning.
- Access AI tools only in line with school guidance and age-appropriate restrictions.

Staff may:

- Use AI tools to support planning, differentiation, and workload, while maintaining professional judgement.
- Model safe, responsible, and transparent use of AI.
- Teach pupils critical thinking skills relating to AI-generated content.

Unacceptable Use

The following uses are not permitted:

- Submitting AI-generated work as original work without acknowledgement (plagiarism).

E-SAFETY POLICY

- Using AI to create harmful, inappropriate, or offensive content.
- Inputting personal, sensitive, or confidential information into AI tools.
- Using AI tools in ways that bypass safeguarding filters or school monitoring systems.
- Using AI for bullying, impersonation, or spreading misinformation.

Data Protection and Privacy

- Users must **not share personal data** (their own or others') with AI platforms.
- Staff must not input identifiable pupil information into AI tools unless approved systems with appropriate safeguards are used.
- The school will ensure compliance with UK GDPR and data protection policies when using any AI technologies.

Safeguarding Considerations

- AI content may be inaccurate, biased, or inappropriate; all users should be encouraged to question and verify outputs.
- Staff must supervise pupil use of AI and respond to any safeguarding concerns arising from its use.
- Any misuse or concerning content generated through AI must be reported following the school's safeguarding procedures.

Academic Integrity

- Pupils must acknowledge when AI tools have been used to support their work, as directed by staff.
- Teachers will provide guidance on appropriate use in assessments and homework.

- The school reserves the right to investigate suspected misuse of AI in line with behaviour and assessment policies.

Education and Awareness

The school will:

- Educate pupils about the opportunities and risks of AI, including bias, misinformation, and ethical considerations.
- Provide staff training on safe and effective AI use.
- Promote digital literacy and critical evaluation of AI-generated content.

Monitoring and Review

- The use of AI will be monitored to ensure compliance with this policy.
- This section will be reviewed regularly to reflect developments in technology and national guidance.