E-Safety, Social Media and Technology Policy

Date approved: **June 2026**
Date for review: **June 2029***

Author: **Anand Marwaha**

*or when required due to changes in laws, technology etc.

Introduction

Wexham School e-safety policy aims to create an environment where student, staff, parents, governors and the wider school community work together to inform each other of ways to use the Internet responsibly, safely and positively.

Through teaching ICT we equip students to participate in a rapidly-changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyse, exchange and present information in a varied and stimulating way. ICT skills are a major factor in enabling them to be confident, creative and independent learners. As the aims of ICT are to equip students with the skills necessary to use technology to become independent learners, the teaching style that we adopt is as active and practical as possible.

Internet technology helps students learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour when achieving this. Students, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour. These agreements and their implementation will promote positive behaviour which can transfer directly into each student's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a list of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer Internet usage and year on year improvement and measurable impact on e-safety. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

E-safety Policy Scope

The school Policy and agreements apply to all students, staff, support staff, external contractors and members of the wider school community who use, have access to or maintain school and school related Internet, computer systems and mobile technologies internally and externally. The school will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and Internet usage both on and off the school site. 'In Loco Parentis' provision under the Children Act 1989 also allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

The e-safety policy covers the use of:

- School based ICT systems and equipment
- School based intranet and networking
- School related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing
- School ICT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets
- Student and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or Internet facilities
- Tablets, mobile phones, devices and laptops when used on the school site.

Managing Information Systems

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and learners.

Local Area Network (LAN), Office 365 and the Staff Shared Drive require robust security measures to protect sensitive information and ensure appropriate access. Access to shared drives should be strictly role-based so that staff can only view or edit files relevant to their professional responsibilities. Highly sensitive data, including safeguarding records, SEN information, and assessment data, must be stored securely with restricted access and appropriate encryption.

Strong password policies, the use of multi-factor authentication (MFA), and regular reviews of user permissions are essential to minimise the risk of unauthorised access or data breaches. In addition, staff should receive regular training on safe digital practices, including identifying phishing attempts, using secure passwords, and managing school data responsibly when working remotely.

Users must act reasonably — e.g., the downloading of large files during the working day will affect the service that others receive.

- Users must take responsibility for their network use. For staff and student breaking our rules of this policy could become a disciplinary issues.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date; through regular patching.
- Virus protection for the whole network must be installed and current.
- Access to the school Wi-Fi is strictly controlled and should not be accessed by students by any wireless devices, any staff that are given permission will be proactively managed and secured.
- Guest Wi-Fi access will be controlled and use monitored.

Wide Area Network (WAN) security issues include:

- Wexham School's broadband firewalls are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between partner organisations.
- The school's broadband network is protected by high performance firewalls.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used unless it has been encrypted and virus checked.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the network will be regularly checked.
- System capacity in relation to storage will be checked regularly.
- The use of user logins and passwords to access the network will be enforced.

Filter Management

- The school's broadband access provides filtering appropriate to the age and maturity of learners. There is flexibility in the filtering system to allow for changes in provision depending on the learning required.
- Any breaches in filtering should be reported to ICT Support and/or emailed to the Headteacher
- If staff or learners discover unsuitable sites, the URL will be reported to the Network Manager who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies.

Monitoring the e-safety policy

The e-safety policy will be actively monitored and evaluated by SLT and the Governing body.

E-safety policy review and evaluation schedule:

- The e-safety policy and Acceptable Use Policy are reviewed at or prior to the start of each academic year and at the point of on-boarding new staff members.

Additionally, the policy will be reviewed promptly upon:

- Serious and/or frequent breaches of the acceptable Internet use policy or other in the light of e-safety incidents.
- New guidance by government / LA / safeguarding authorities.
- Significant changes in technology as used by the school or pupils in the wider community.
- E-safety incidents in the community or local schools which might impact on the school community.
- Advice from the Police and/or the Slough Safeguarding Partnership.
- In line with OFSTED recommendations, it is also useful to consult with students over the policy and to ask for their opinion on keeping themselves self when using the Internet.

School Management and e-safety

The SLT is responsible for determining, evaluating and reviewing e- safety policies to encompass teaching and learning, use of school IT equipment and facilities by students, staff and visitors, and the agreed criteria for acceptable use by students, school staff and governors of Internet capable equipment for school related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

The e-safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, and partnership discussion with stakeholders and outside organisations;

- technological and Internet developments, current government guidance and school related e-safety incidents

- the policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine inset provision for staff and governors and guidance provided to parents, pupils and local partnerships
- e-safety provision is always designed to encourage positive behaviours and practical real-world strategies for all members of the school and wider school community
- the leadership team is encouraged to be aspirational and innovative in developing strategies for e-safety provision.

The school e-safety Coordinator:

The school has a designated e-safety Coordinator who reports to the SLT and Governors and coordinates e-safety provision across the school and wider school community.

- The school's e-safety coordinator is the Assistant Headteacher i/c T&L.
- The school e-safety coordinator is responsible for e-safety issues on a day to day basis and also liaises with LA contacts, filtering and website providers and school ICT support.
- The school e-safety coordinator where required maintains a log of submitted e-safety reports and incidents.
- The school e-safety coordinator audits and assesses inset requirements for staff, support staff and Governor e-safety training, and ensures that all staff are aware of their responsibilities and the school's e-safety procedures. The coordinator is also the first port of call for staff requiring advice on e-safety matters.
- Although all staff are responsible for upholding the school e-safety policy and safer Internet practice, the e-safety Coordinator, the Head Teacher and the Network Manager are responsible for monitoring Internet usage by students and staff, and on school machines, such as laptops, used off-site.
- The e-safety Coordinator is responsible for promoting best practice in e-safety within the wider school community, including providing and being a source of information for parents and partner stakeholders.
- The school e-safety coordinator (along with IT support) should be involved in any risk assessment of new technologies, services or software to analyse any potential risks

Governors' responsibility for e-safety

- At least one Governor is responsible for e-safety, and the school e-safety Coordinator will liaise directly with the Governor with regard to reports on e-safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community. The e-safety coordinator will be responsible for auditing Governor safety training and inset requirements.

ICT support staff and external contractors

- External ICT support staff and technicians are responsible for maintaining the school's networking, IT infrastructure and hardware. They are aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet is secure. They further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
- Support staff maintain and enforce the school's password policy.

- External contractors, such as VLE providers, website designers/hosts/maintenance contractors are made fully aware of and agree to the school's e-safety Policy. Where contractors have access to sensitive school information and material covered by the Data Protection Act, for example on a VLE, school website or email provision, the contractor should also be DBS checked. A Service Level Agreement (SLA) is in place with the Local Authority to provide school standard provision and support.

Teaching and teaching support staff

- Teaching and teaching support staff need to ensure that they are aware of the current school e-safety policy, practices and associated procedures for reporting e-safety incidents.
- Teaching and teaching support staff will be provided with e-safety induction as part of the overall staff induction procedures.
- All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the Acceptable Use Agreement relevant to Internet and computer use in school.
- All staff need to follow the school's social media policy, in regard to external off site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on Internet school messaging or communication platforms, for example email, VLE messages and forums and the school website.
- All teaching staff need to rigorously monitor student internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site.
- Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
- Be aware of online propaganda and help pupils with critical evaluation of online materials.
- Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with learners or parents/carers is required, such as on a residential field trip.
- In school mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless absolutely required.
- If members of staff have an educational reason to allow student to use mobile phones or personal device as part of an educational activity then this is acceptable.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of learners and will only use work-provided equipment for this purpose. Some exceptions may apply if permission is given by the Headteacher, for example our Twitter Champions or to capture and promote high-quality T&L. Should this be the case all school related recordings or imagery must be deleted from the device as soon as possible.
- If a member of staff breaches the policy then disciplinary action may be taken.

Designated Safeguarding Officer

- The Designated Safeguarding Officer is trained in specific e-safety issues. Accredited training with reference to child protection issues has been accessed.
- The Designated Safeguarding Officer can differentiate which e-safety incidents are required to be reported to CEOP, local Police, LADO, Local Safeguarding Children's Board, social services and parents; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.
- Possible scenarios might include:
    a) Allegations against members of staff.
    b) Computer crime – for example hacking of school systems.
    c) Allegations or evidence of 'grooming'.
    d) Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.
    e) Producing and sharing of Youth Produced Sexual Imagery (YPSI)
- Acting 'in loco parentis' and liaising with websites and social media platforms such as X, Instagram, Snapchat and Facebook to remove instances of illegal material or cyber bullying.

Students

Are required to use school Internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies. Students are expected to sign the policy to indicate agreement, and/or have their parents/carers sign on their behalf.

- Students need to be aware of how to report e-safety incidents in school, and how to use external reporting facilities, such as the Click CEOP button or Childline number.
- Students need to be aware that school Acceptable Use Policies cover all computer, Internet and mobile technology usage in school, including the use of personal items such as phones.
- Students need to be aware that their Internet use out of school on social networking sites such as Instagram is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and students in terms of cyber bullying, reputation, or illegal activities.

Students Use of Personal Devices

Wexham School recognises how important technology is and that parents and students may well want their mobile phones with them for personal safety on the way to and from school. Therefore, students in Years 7-11 are allowed mobile phones in school BUT they must be switched off and kept out of site at all times. This will change in September 2026 or earlier when the school invests in pouches in order to legally comply with government guidance.

Years 12 and 13 are allowed phones but they must not be used whilst circulating the school in order to set a good example to younger students. Headphones are not permitted in school and therefore should not be seen.

Mobile phones and headphones will be confiscated if the above is not followed and will be kept securely in school for a minimum of 24 hours, after which only a parent or carer may collect them from the main school office. Frequent flouting of this rule will result in other sanctions for defiance and the total ban of any mobile phone device being brought to school.

In addition, for all students

- Phones and devices must never remain on their person in examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body and this would result in the student's withdrawal from that examination or all examinations.
- If a student's needs to contact their parents or carers they are encouraged to use a school phone.
- Parents/Carers are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Children and young people should protect their phone numbers by only giving them to trusted friends and family members.
- The school does not accept any liability for loss, damage or theft of mobile phones if they are brought to school by students.

Parents and Carers

- Parents and carers should support the school's stance on promoting good internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.
- Parents and carers must sign the School's Acceptable Use Agreement, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as extranets, websites, forums, social media, online reporting arrangement, questionnaires and the VLE.
- The school will provide opportunities to educate parents with regard to e-safety through the school website and contact points.

Other users

- Other users such as school visitors, or wider school community stakeholders or external contractors should be expected to agree to a visitor's level of access and usage.
- External users with significant access to school systems including sensitive information or information held securely under the Data Protection Act should be DBS checked. This includes external contractors who might maintain the school domain name and web hosting – which would facilitate access to cloud file storage, website documents, and email.

The school's provision of e-safety education

'Teaching online safety in school (DfE, June 2019) outlines the importance of schools helping children and young people not only use the internet safely, but also give them opportunities to learn how to behave online. Through Relationships and Sex Education and Health Education students will be taught what positive, healthy and respectful online relationships look like.

The PSHE curriculum will deliver and underpin key knowledge and behaviours:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Online behaviour
- How to identify online risks
- How and when to seek support

Throughout the curriculum, teaching about potential harms will include:

- Age restrictions
- Content: How it can be used and shared
- Disinformation, misinformation and hoaxes
- Fake websites and scam emails
- Fraud (online)
- Password phishing
- Personal data
- Persuasive design which keeps 'users online for longer than they might have planned or desired'
- Privacy settings
- Targeting of online content
- Abuse (online)
- Challenges [to do something and post about it)
- Content which incites e.g. hate speech, violence
- Fake profiles
- Grooming
- Live streaming
- Pornography
- Unsafe communication
- Impact on confidence (including body confidence)
- Impact on quality of life, physical and mental health and relationships
- Online vs. offline behaviours
- Reputational damage
- Suicide, self-harm and eating disorders

E-safety is accessed as part of pastoral care during form time activities, assemblies, year group presentations, tutorial opportunities. It is formally taught through the PSHCE curriculum and in other subject curriculum wherever relevant.

Parents/Carers – information and events

- E-safety information is directly available to parents via the school website which is updated with the latest E safety news and issues.

- School subscribes to a dedicated E-safety support platform. School will take advantage of occasions when there are large numbers of parents in school to promote e safety.

Staff – inset and training

- A planned programme of e-safety training opportunities is available for staff, including on site inset, whole staff training, online training opportunities (for example E-safety Support courses), external CPD courses, accredited CPD courses, (for example CEOP) and Coordinator training.
- The E-safety Coordinator should be the first port of call for staff requiring E-safety advice.

Governors

- E-safety information will be directly delivered to governors via the E-safety Coordinator.
- Governors will be provided access to specific governor training provided externally by the LA through the Governors training programme.

ICT support staff – contractors, filtering and monitoring

- IT support staff and contractors will ensure that bought in hardware and software solutions feature built in training provision
- Support staff and contractors will be DBS checked and agree and sign the school's e-safety acceptable user's agreement.
- IT technical support staff and network managers have relevant industry experience and Microsoft/Cisco certified qualifications.

Legal Information

Policy guidance for handling personal data, dealing with freedom of information requests, and complying with privacy regulations pertaining to website data: All of these areas are regulated by the Information Commissioner (ICO), and every UK organisation has to comply with the responsibilities and obligations as defined by the ICO. Schools are no different to any other organisation in this regard. The ICO guidance on how to comply with these obligations is updated regularly. The School will refer directly to this guidance in these areas.

When disposing of computer equipment we will ensure all data, including personal data is wiped, not deleted from storage.

Use of IT facilities for curriculum teaching and learning: Use of the Internet and IT facilities should be clearly planned prior to the activity. Websites and software Apps should be suggested, Students should be trusted to be responsible when researching the Internet, and teaching staff will consider the age and maturity of the students.

General Data Protection and e-safety

The GDPR sets out the key principles that all personal data must be processed in line with.

- Data must be: processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected

There are also stronger rights for individuals regarding their own data.

- The individual's rights include: to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all.
- The General Data Protection Act is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.
- Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies. Personal and sensitive information should only be sent by e mail when on a secure network. Communication with external agencies will for sensitive data will be via our EGRESS system.
- Personal data should only be stored on secure devices. In other words, only computers, servers, file- servers, cloud space, or devices which require a user name and password to access the information.
- Secure accounts need to be logged off after use to prevent unauthorised access.
- Personal e mails should not be used for school business and likewise school email accounts must not be used for personal business.

Personal information on the school website

- No material defined as 'personal information' under the General Data Protection Act will be used on the school website.
- The school considers staff privacy issues carefully with regard to publishing staff email addresses, staff lists, photos of staff, staff qualifications and any other personally identifying information.

E-safety and the Law

This E-safety policy takes into the following legislation;

a) The Education and Inspections Act 2006 (Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the school behaviour policy.)
b) Computer Misuse Act 1990, sections 1-3
c) Data Protection Act 2018
d) General Data Protection Regulations
e) Freedom of Information Act 2000
f) Communications Act 2003 section 1,2
g) Protection from Harassment Act 1997
h) Regulation of Investigatory Powers Act 2000
i) Copyright, Designs and Patents Act 1988
j) Racial and Religious Hatred Act 2006
k) Protection of Children Act 1978 Sexual Offences Act 2003

Schools have a 'duty of care' to pupils, and as such act 'in loco parentis.' Under the Children Act 1989, this enables schools to remove personal information, cyber bullying and comments relating to school pupils as if they were the child's parent. Facebook in particular has provision for using 'in loco parentis' when reporting cyber bullying. This is relevant to all schools.

Useful links to external organisations:

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact local Police.

Kidsmart: www.kidsmart.org.uk

Keeping Children Safe in Education (KCSIE) 2025

Appendix

Key Principles

- All staff at Wexham School have a responsibility to ensure that they protect the reputation of the school, and to treat colleagues with professionalism and respect.
- It is important to protect everyone at Wexham School from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding children is a key responsibility and priority of all members of staff and it is essential that everyone at Wexham School considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking. Any social media contact with any child under the age of 18 who is a current or former pupil other than a child who is related to them (e.g. a son or daughter) is not permitted.

Use of Social Media in practice School-sanctioned use of social media

- There are many legitimate uses of social media to support school marketing and public relations activities. For example, the school has an official X account.
- Before creating a social media account, the school should carefully consider appropriate social media channels, the purpose for using them and where necessary seek advice.

The school should also adhere to these guidelines:

1. The content of any school-sanctioned social media site should be solely professional and should reflect well on the school.
2. All content should adhere to the school's ethos and be reflective of core values.
3. Appropriate privacy settings should be set that disallow others to post to a school's social media page or require approval of posts. Age restrictions should also be set to at least 13+ and where applicable a profanity filter should be applied, for example, on Facebook.
4. Staff must not publish photographs of children without the written consent of parents / carers (this is held on SIMs)
5. Identify by name any children featured in photographs, or allow personally identifying information to be published on school social media account.
6. Parents and staff should be informed of any new social media sites that are created.
7. Care must be taken that any links to external sites from the account are appropriate and safe
8. Any inappropriate comments on or abuse of school-sanctioned social media should immediately be removed and reported to a senior member of staff
9. All official school social media accounts should be regularly monitored and maintained.
10. Any serious incidents which may damage the reputation of the school, or particular student, member of staff or other individual should be immediately reported to the Headteacher.
11. Students under the age of 13 should not be allowed access to, or be encouraged to create their own personal social media accounts. Children under the age of 13 are not legally allowed to use social media channels such as Facebook and X. However, students may be encouraged to observe official school social media profiles in an appropriate and safe way, for example, via a feed on the school's website.
12. The Headteacher has responsibility for running the school's official website and X site. No other social media platforms may be set up by any member of the whole school community without permission from the Headteacher.

13. Whilst parents, staff and the wider school community are encouraged to interact with these social media sites they should do so with responsibility and respect.
14. Complaints should not be dealt with via social media and should be diverted to an appropriate communications channel.
15. Staff, parents and the wider school community should not edit open access online encyclopaedias such as Wikipedia in a personal capacity. The source of the correction will be recorded and Wexham School reserves the right to amend these details for their sole purpose.
16. All staff who wish to engage with a school's social media platforms are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. All staff should keep their passwords confidential, change them often and be careful about what is posted online.
17. Parents and the wider school community should not post images or videos from school events on any public social media site. Images or videos taken at school events, when such permission has been granted by the school, are for the sole and private use of that individual and their use must be in accordance with the Data Protection Act 2018.
18. Any communication received from children on any personal social media sites must be reported to the designated person for Child Protection.
19. If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
20. All email communication between staff and members of the school community on school business must be made from an official school email account.
21. Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Headteacher.
22. Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.
23. Staff should not comment on the school's official social media page from their personal account.
24. Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts.
25. Staff should not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, and subscriber or similar on any personal social media account, with the exception of relatives.

In addition to the above everyone at Wexham School must ensure that they:

- Communicate with children and parents in an open and transparent way using the school phone number and email address
- Never 'friend' a pupil at the school onto their social networking site.
- Are conscious at all times of the need to keep personal and professional/school lives separate. Individuals should not put themselves in a position where there is a conflict between the school and their personal interests.
- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.
- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school's reputation is compromised by inappropriate postings.

Principles – Be Responsible and Respectful

- Users should not engage in activities involving social media which might bring Wexham School into disrepute.
- Users should not represent their personal views as those of Wexham School on any social medium
- Users should not discuss personal information about other students, Wexham School and the wider community they interact with on any social media.
- Users should not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations or Wexham School.
- Staff should not identify themselves as members of Wexham School in their personal web-space, unless specifically linked to an approved job role within the school community where it serves a purpose to professionally market the school or wider trust. This is to prevent information being linked with the school and to safeguard the privacy of staff members, students and parents and the wider school community.
- Students should not have contact through any personal social medium with any member of staff. If students and members of the wider school community wish to communicate with staff they should only do so through official school sites created for this purpose.
- Photographs, videos or any other types of images of pupils and their families or images depicting staff members, clothing with school logos or images identifying school premises should not be published on personal or public web space without prior permission from the school.

Personal use of social media

- Under no circumstances should staff make reference to any staff member, student, and parent or school activity/event. The following are also not considered acceptable Wexham School: The use of the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.
- Wexham School accepts that some sites may be used for professional purposes to highlight a personal profile with summarised details, e.g. LinkedIn and Twitter. The school would advise that care is taken to maintain an up to date profile and a high level of presentation on such sites if Wexham School is listed.
- Staff who run blogging/microblogging sites, which have a professional and/or educational status are advised to seek guidance and advice from the Headteacher regarding prudence and endorsement of views if there is any link referencing Wexham School.
- School staff should not invite, accept or engage in communications with parents or children from the school community in any personal social media whilst in employment at Wexham School.

Safer Online Behaviour

In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for students or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, children or other individuals connected with the school, could result in formal action being taken against them. This includes the uploading of photographs which might put the school into disrepute.

Student Conduct

- As members of the School community, students must abide by the expectations of the school code of conduct, respecting the rights of fellow students and staff, as well as the reputation of the School. They should think carefully about how they express themselves. Material posted on the internet can be hard to delete and should, therefore, be considered permanent.
- Students must not post comments on a social networking site or blog, or send text messages:
    - That could be viewed as bullying or harassment of another member of the school community.
    - That are counter to the Schools Equality and Diversity policy.
    - That explicitly encourages other members of the school community to break the law.
    - That are likely to bring the school into dispute.
- Students should not post photos that they do not wish others to see.
- Students should not invite staff to join social networks or follow purely personal profiles.
- Students will be given guidance on appropriate use of the internet and e-safety through tutorial and displays.
- If a student has a cause for concern regarding use of the internet or social networking, they must report the incident immediately to a member of staff. There may be occasions where this will be treated as a safeguarding issue.

Artificial Intelligence (AI) Risks and Safeguarding

With the increasing use of Artificial Intelligence (AI) technologies in education and online platforms, Wexham School recognises the need to address emerging risks associated with AI-generated content and tools.

Potential Risks

- Deepfakes and synthetic media: AI can create realistic but fake images, videos, or audio that may be used for bullying, harassment, or reputational damage.
- Misinformation and disinformation: AI-generated text and media can spread false information quickly, influencing opinions and causing harm.
- Automated grooming or exploitation: AI-driven chatbots or platforms may be misused to target vulnerable individuals.

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. The 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. The school will treat any use of AI to bully students in line with our Anti-Bullying Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Guidance for Staff and Students

- Staff must ensure that any AI tools used for teaching and learning are approved by the school and comply with data protection and safeguarding standards.
- Students should be educated on how to critically evaluate AI-generated content and report suspicious or harmful material.
- Regular staff training will include awareness of AI risks, detection of synthetic media, and strategies for promoting safe and responsible AI use in education.

Monitoring and Reporting

- The school will monitor the use of AI tools within its network and ensure filtering systems are updated to detect harmful AI-generated content.
- Any incidents involving AI misuse must be reported immediately to the Designated Safeguarding Lead (DSL) and recorded in line with safeguarding procedures.

This section aligns with Keeping Children Safe in Education (KCSIE) 2025 guidance, which emphasises the importance of addressing emerging technologies in safeguarding policies.