ST JOHN PAYNE CATHOLIC SCHOOL

E-Safety and AI POLICY

Guidance Policies for ICT Acceptable Use

POLICY LEAD	Mr P Marsh and Mr C de Vries School SIRO: Mr T Coen
APPROVED BY	Full Governing Body
APPROVAL DATE	November 2026
IMPLEMENTATION DATE	November 2026
REVIEW DATE	November 2027
NOMINATED COMMITTEE	Full Governing Body
POLICY STATUS	Statutory

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources, including AI, web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within society as a whole.

At St John Payne Catholic School we understand the responsibility to educate our pupils on eSafety issues. We teach them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties. Even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet technologies.

Filtering and Monitoring

Authorised ICT staff, and authorised members of the Senior Leadership Team, may inspect school-owned or leased equipment and access or monitor school systems and communications for a defined, lawful purpose where this is necessary and proportionate. Staff should refer to the school's privacy notice for details.

Monitoring or access may be undertaken for the following purposes:

- To confirm or obtain school business related information.
- To confirm or investigate compliance with school policies, standards and procedures.
- To ensure the effective operation of School ICT.
- For quality control or training purposes.

- To respond to subject access requests under Article 15 of the UK GDPR and Data Protection Act 2018

- To prevent or detect crime.

Authorised staff may access the school email or voicemail of an absent staff member where this is necessary and proportionate to deal with school business.

Monitoring and investigations are carried out by authorised staff in accordance with the UK GDPR and the Data Protection Act 2018.

Monitoring of school systems may incidentally capture personal communications.

Managing Filtering and Monitoring Systems

Our school is committed to meeting the Department for Education's standards for filtering and monitoring to ensure a safe and secure online environment for all students and staff. We have clearly assigned roles and responsibilities to ensure effective oversight and implementation. A designated member of the Senior Leadership Team (SLT) and a named governor are responsible for ensuring compliance with statutory requirements. The SLT oversees the procurement of appropriate filtering and monitoring systems, documents decisions regarding what content is blocked or allowed, and regularly reviews the effectiveness of these systems. All staff are trained to understand their responsibilities, follow established procedures, and respond appropriately to any concerns. This structured approach ensures that our filtering and monitoring provision is not only compliant but also proactive and responsive to emerging risks.

The Designated Safeguarding Lead (DSL) plays a central role in leading on safeguarding and online safety, including reviewing monitoring reports, responding to concerns, and providing assurance to governors that systems are functioning effectively. Our IT support whether in-house or through a third-party provider is responsible for the technical maintenance of filtering and monitoring systems, generating reports, and implementing any necessary actions following system checks or concerns. The DSL, SLT, and IT support work collaboratively to identify risks, carry out regular reviews, and ensure that systems remain up to date and effective. This coordinated effort ensures that we meet all key requirements: assigning clear responsibilities, maintaining effective systems, documenting decisions, training staff, and regularly reviewing and improving our provision in line with statutory guidance such as *Keeping Children Safe in Education*.

Reviewing Filtering and Monitoring Provision

As part of our commitment to maintaining a safe digital environment, the school conducts an annual review of its filtering and monitoring systems to ensure they remain effective, up to date, and aligned with statutory safeguarding requirements. The review includes an evaluation of system performance, analysis of filtering and monitoring reports, and a reassessment of what content is blocked or allowed based on current risks and educational needs. All manual changes to the filtering rules are documented and any necessary adjustments are implemented promptly.

Our third-party software provider plays a key role in supporting this review by supplying detailed reports, conducting system checks, and reacting to best practices and emerging threats. Their expertise ensures that technical requirements such as system maintenance, risk identification, and performance monitoring are consistently met to a high standard. The school uses these insights to assess safeguarding implications and provide assurance to governors that the systems are functioning effectively.

Filtering Systems and Teaching and Learning

Our filtering solution is tailored to different user groups such as students and staff ensuring age-appropriate access while supporting teaching and learning. The system is regularly updated to block harmful and inappropriate content without placing unreasonable restrictions on educational activities or administrative functions. We ensure that blocklists from the Internet Watch Foundation (IWF) and the Counter-Terrorism Internet Referral Unit (CTIRU) are integrated and cannot be disabled, and our provider is a registered member of both organisations.

Our third-party provider also supports us in meeting the technical requirements of the standard, including filtering across all school-managed devices, BYOD schemes, and guest access. The system is capable of identifying users, devices, and search terms, and provides alerts for concerning activity. It blocks circumvention tools such as VPNs and proxies, and is configured to filter multilingual content, images, and common misspellings. We ensure safe search is enforced across browsers and that unauthorised plugins or browsers cannot be installed. Staff are trained to report any concerns, including access to unsuitable material, software failures, or filtering issues that affect learning. We also conduct Data Protection Impact Assessments (DPIAs) and review privacy notices in line with ICO guidance.

Safeguarding and Monitoring Strategies

Monitoring alerts are configured to flag high-risk incidents immediately, while weekly reports provide a broader overview of user activity. All users are made aware that

monitoring is in place, and clear guidance is provided to staff on how to respond to incidents in line with our safeguarding policies.

Our third-party provider ensures that monitoring systems are active, effective, and capable of identifying concerning behaviours across all school-managed devices, including mobile and app-based content. The system provides detailed, user-identifiable reports that include device information, timestamps, and the nature of the content flagged. IT support staff, trained in safeguarding and online safety, manage the technical aspects of monitoring and report concerns directly to the Designated Safeguarding Lead (DSL).

Our monitoring procedures are reflected in our Acceptable Use Policy (AUP) and safeguarding documentation.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the Essex County Council Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Report suspected cyber or IT security incidents immediately to the Network Team. This includes phishing, lost or stolen devices or data, suspected account compromise, malware and unauthorised access or use. The Network Team will escalate to the Senior Information Risk Owner (SIRO) as appropriate.

Report online safeguarding concerns immediately to the Designated Safeguarding Lead (DSL), following the school's safeguarding procedures.

Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet, telephone and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its

contents. Any concerns or clarification should be discussed with the school eSafety coordinator or Headteacher, the Senior Information Risk Owner.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software e.g. SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal
- data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not physically move to another location or make changes to any hardware without permission from Network Manager.
- I will not purchase / install any hardware or software without permission from the Network Manager.
- I will notify the Network Team at the nearest opportunity of any damage to any network equipment that I discover.
- I will immediately notify the network team or the Network Manager if I feel that my secure login (password) has been compromised or if I believe I have contracted a computer virus.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full via our publications scheme on our website.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…… Date ……

Full Name …….....(printed)

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media must be checked for any viruses using school provided anti-virus software before using them.
- Never interfere with any anti-virus software installed on school ICT equipment that you use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.
-

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.

- Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO) (Network Manager and Site Manager).
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- When travelling staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned, emailed or printed.

Information Asset Guardian

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Schools should identify an Information Asset Owner. For example, the school's Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manager could be the Information Asset Guardian.

The role of an IAG is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DCSF number, etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

As a result, the IAG is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several IAGs, whose roles may currently be those of e-safety coordinator, ICT manager or Management Information Systems administrator or manager.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised means only. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- Use secure erasure or destruction method appropriate to the storage media and retain a record of disposal. Use only authorised companies that provide written evidence of secure erasure or destruction.
- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal .
- The school's disposal record will include:
  - Date item disposed of
  - Authorisation for disposal
  - How it was disposed of e.g. waste, gift, sale
  - Name of person & / or organisation who received the disposed item
- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check.

e-Mail

The use of e-mail within schools is an essential means of communication for staff, parents and pupils. In the context of school, e-mail messages are the property of the school and should not be considered private.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is logged; if necessary

email histories can be traced. The school email account should be the account that is used for all school business.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending e-mails to external organisations, parents or pupils are to cc. the Headteacher, line manager or designated account if appropriate. Staff to seek clarification from line manager if unsure.
- Pupils may only use school approved accounts on the school system and only for educational purposes.
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Users should therefore actively manage their e-mail account as follows:
    - Manage emails in line with the school's retention schedule.
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All pupil e-mail users must not reveal any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the ICT Scheme of Work.
- However, you access your school e-mail (whether directly, through webmail when away from the office/classroom or on non-school hardware) all the school e-mail policies apply.

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data, please adhere to the points below:

- Verify the details, including accurate e-mail address, of any intended recipient of the information.
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not identify such information in the subject line of any e-mail
  Request confirmation of safe receipt
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Avoid unnecessary attachments. Share files using approved school storage and check who can open the link before sending.
- School e-mail is not to be used for personal advertising
- All emails sent should be courteous and polite and adhere to the guidance below:

1. Make sure your e-mail includes a courteous greeting and closing.
2. Address your contact with the appropriate level of formality and make sure you spelled their name correctly.
3. Read your email out loud to ensure the tone is that which you desire. A few additions of the words "please" and "thank you" go a long way.
4. Use sentence case.
5. Just because someone doesn't ask for a response doesn't mean you ignore them. Always acknowledge emails from those you know in a timely manner.
6. Keep emails brief and to the point.

Receiving e-Mails

- Email is a vital method of communication within the school. It is therefore expected that staff will check their email regularly (at least once per day as a minimum).
- Activate your ‘out-of-office’ notification when away for extended periods
- Use the ‘Delegation’ facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (see the Network Team to enable this).

- Never open attachments from an untrusted source; Consult your network manager first.
- Do not use the email systems to store attachments. Save business related files to the appropriate location in approved school storage.

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil experiences difficulty with social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

eSafety

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in ICT/ PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.

- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety issues in the form of staff Inset training.

- New staff receive information on the school's acceptable use policy as part of their induction.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community).

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Incident Reporting, eSafety Incident Log & Infringements

For reporting routes, see Incident Reporting on page 5.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety coordinator or Headteacher.

Inappropriate Material

- Report accidental access to inappropriate material immediately using the reporting routes on page 5.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- Staff will preview any recommended sites, including video clips, before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Social Media and Social Networking Technologies

Social Media and social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school .

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/ carers are required to decide as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- Parents/carers are expected to sign a Home School agreement on admission to school.
- The school disseminates information to parents relating to eSafety where appropriate.

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer-based services
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file

- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

Remote Access

- You are responsible for all activity via your remote access facility.
- Only use equipment with an appropriate level of security for remote access.

  Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment.

Safe Use of Images

Taking of Images and Film

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils provided the image is captured using a device which is property of the school.
- Staff can only use personal digital equipment, such as mobile phones and cameras, to record images of pupils with the express permission of the Headteacher or eSafety Coordinator. Images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

Mobile Technologies

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device without permission from the Headteacher.
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes. At all times the device must be switched onto silent .
- This technology may be used, however, for educational purposes, as mutually agreed with the Headteacher or eSafety Coordinator. The device user, in this instance, must always ask the prior permission of the bill payer .
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device .

Servers

- Newly installed servers holding personal data should be encrypted, therefore password protecting data.
- Always keep servers in a locked and secure environment.
- Limit access rights to ensure the integrity of the standard build.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine's specification.
- Data must be backed up regularly. Backup media must be encrypted and stored securely in line with the school's IT backup procedure.
- Back up media stored off-site must be secure.
- Remote backups should be automatically securely encrypted.
- Regular updates of anti-virus and anti-spyware should be applied.
- Records should be kept of when and which patches have been applied.

- Ensure that web browsers and other web-based applications are operated at a minimum of 128 BIT cipher strength.

Writing and Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them.

This policy will be reviewed annually and consideration given to the implications for future whole school development planning and to ensure it reflects current technology, legal standards, and best practices in education. Input from students, parents, and staff will be considered to keep the policy responsive to the needs of the school community.

Artificial Intelligence (AI) Policy

This policy applies to all students and staff at St John Payne Catholic School. It covers the use of AI on school devices and networks. This includes personal devices if used for school-related tasks.

Responsible AI Use for Educational Purposes

AI should be used solely to support learning, skill development, and administrative efficiency. Non-educational or personal use of AI on school devices and networks is prohibited.

Academic Integrity & Transparency in Use

Unless specifically permitted, students may not use AI for homework or coursework. All work produced for external assessment, e.g. coursework, must be completed adhering to the JCQ AI Use in Assessment Policy .

Departments must educate students in appropriate use of AI and risks of misuse. Students submitting non-examination assessment (NEA) will sign a declaration that they have adhered to requirements and must be able to demonstrate their submission is the result of their independent work and thought.

Plagiarism and Accuracy

Submitting AI generated work without proper citation is considered plagiarism. An appropriate department sanction could be to complete the work in detention. Parents should be informed if students have been found to submit a piece of AI generated work that they have claimed to be their own.

Examples of AI misuse include, but are not limited to:

- Copying or paraphrasing sections of AI generated content so that the work submitted for assessment is no longer the student's own.
- Copying or paraphrasing whole responses of AI-generated content.
- Using AI to complete parts of the assessment so that the work does not reflect the student's own work, analysis, evaluation or calculations.
- Failing to acknowledge use of AI as a source of information.
- Incomplete or poor acknowledgement of AI.
- Submitting work with intentionally incomplete or misleading references or bibliographies.

AI can generate images and text which can be factually inaccurate or offensive. Students will be responsible for any content submitted.

Potential Indicators of AI Misuse

If the following are seen in student work, it may be an indication the student has misused AI:

a) A default use of American spelling, currency, terms and other localisations.

b) A default use of language or vocabulary which may not accord with the qualification level (though be aware AI tools may be instructed to employ different languages, registers and levels of proficiency when generating content).

c) A lack of direct quotations and/or use of references where these are required/ expected (though some AI tools will produce quotations and references).

d) Inclusion of references which cannot be found or verified (some AI tools have provided false references to books or articles by real authors).

e) A lack of reference to events occurring after a certain date (reflecting when an AI tool's data source was compiled), which may be notable for some subjects.

f) Instances of incorrect and/or inconsistent use of first-person and third-person perspective where generated text is left unaltered.

g) A difference in the language style used when compared to that used by a student in the classroom or in other previously submitted work.

h) A variation in the style of language evidenced in a piece of work, if a student has taken significant portions of text from AI and then amended it.

i) A lack of graphs/data tables/visual aids where these would normally be expected.

j) A lack of specific local or topical knowledge.

k) Content being more generic in nature rather than relating to the student, or a specialised task or scenario, if this is required or expected.

l) The inadvertent inclusion by students of warnings or provisos produced by AI to highlight the limits of its ability, or the hypothetical nature of its output.

m) The submission of student work in a typed format, where their normal output is handwritten.

n) The unusual use of several concluding statements throughout the text, or several repetitions of an overarching essay structure within an essay, which can be a result of AI being asked to produce an essay several times to add depth and variety or to overcome its output limit.

o) The inclusion of strongly stated non-sequiturs or confidently incorrect statements within otherwise cohesive content.

p) Overly verbose or hyperbolic language not consistent with the candidate's usual style.

Strategies that staff could use to identify AI use include:

- AI checking software.
- Comparing with previous work. Has there been a significant change in quality? Where appropriate, set a controlled assessment at the beginning of the course for students to complete in class.
- Discussing verbally the submitted work with the student to check understanding
- Look for indicators of AI misuse. See section 9.

Bias Awareness

Teachers and students should be aware that AI models may carry biases. AI should be used critically.

Data Privacy and Security

Personal Data Protection

No personal or school data must be uploaded into an external AI tool in line with GDPR regulations. This includes names and addresses**.**

Staff will receive ongoing training on how to integrate AI into their teaching ethically and effectively.

Lesson Planning, Student Feedback and Marking & Assessment

Staff must be transparent and role model good practice where AI is used to produce resources, and students must be informed if AI has been used to mark their work.

Whilst AI can assist staff workload and wellbeing with regards to marking and assessment, teachers must maintain direct and personal awareness of students' abilities. Teachers must guard against the potential of students feeling that teachers have delegated personal interest in their efforts.

External Communication

To preserve our positive partnerships with families and protect staff and the school from reputational damage, staff must not use AI for external communication other than to check spelling and grammar. All communication particular to individual students must remain authentic and personal.

This includes notes detailing behaviour incidents on SIMs and Edulink as these must be particular to the incident, and statements must be personal and first hand.

AI can be used for generic correspondence such as letters detailing extra-curricular opportunities.

Safeguarding Reporting: My Concern

AI must not be used to detail any safeguarding report.

Feedback and Reporting

Staff, students and parents are encouraged to report any concerns about AI use or its impact on learning and privacy. The school will review and address these concerns as required.