Kendrick School

Internet and E-safety Policy for Staff

Approval Date: September 2023

Next Review Date: June 2025

Version: IESP:V1 2019	
Version: IESP: V2 2021	
Version: IESP: V3 2023	

Internet and E-safety Policy for Staff

Kendrick School Internet and E-mail Access

This policy must be read in conjunction with Kendrick School's Inclusion Policy and Safeguarding Policy, Relationships and Behaviour Policy, Child Protection and Safeguarding Policies and Anti-Bullying policies.

Whole School Policy

1. **Introduction**

   Importance of the Internet and E-mail to schools
   The School's Internet and E-Safety Policy reflects the importance it places on the safe use of information systems and electronic communications by staff and students. E-Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate staff, governors and students about the benefits, risks and responsibilities of using information technology.

   - e-Safety concerns safeguarding staff and students in the digital world.

- e-Safety emphasises learning to understand and use new technologies in a positive way.
- e-Safety is less about restriction and more about education about the risks as well as the benefits so all can feel confident online.
- e-Safety is concerned with supporting staff and students to develop safer online behaviours both in and out of school.

Staff and students need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. Schools have a duty of care to enable students to use on-line systems safely and staff are suitably trained to delivering their Learning and Teaching with e-safety in mind.

The rapid development and accessibility of the Internet and new technologies such as personal publishing, AI, and social networking means that e-Safety is an ever growing and changing area of interest and concern. The school's e-Safety policy reflects this by keeping abreast of the vast changes taking place.

.

An E-safety group has been formed to:

- To ensure that E-safety awareness is high priority in the school.
- To monitor internet use by staff and students.
- To ensure Ofsted guidelines are adhered to.
- Liaise with parents and students.
- Ensure E-safety is part of the curriculum.

2. Scope of the Policy

This policy applies to all members of Kendrick School (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Kendrick School IT systems, both in and out of Kendrick School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

Kendrick School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school

3. Roles and Responsibilities

The school's Internet and E-Safety Coordinator is the Assistant Headteacher –AHT1
The school's Internet and E-Safety Governor is tbc.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety
- reporting to relevant Governors

Headteacher and Senior Leadership Team

• The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.

• The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See "Responding to incidents of misuse" other relevant body disciplinary procedures).

• The Headteacher/Senior Leadership Team are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

• The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

• The Senior Leadership Team/Head's PA/ Key stage pastoral leaders will receive regular monitoring reports from Securely which produces reports on potential student misuse. These are followed up with student/staff concerned

E-Safety Coordinator:

• leads on e-safety issues
• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
• ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
• provides training and advice for staff
• liaises with relevant bodies
• liaises with school technical staff
• receives reports of e-safety incidents and files a log of incidents to inform future e-safety developments
• meets regularly with E-Safety Governor to discuss current issues
• attends relevant meeting/committee of Governors
• reports regularly to Senior Leadership Team

Network Manager:

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required e-safety technical requirements and any other relevant body E-Safety Policy/Guidance that may apply

- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that monitoring software are implemented and updated as agreed in school policies.

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Agreement .
- they report any suspected misuse or problem to the Headteacher/E-Safety Coordinator for investigation/action/sanction.
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other activities.
- students understand and follow the e-safety and acceptable use agreements.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

Students:

- are responsible for using the school IT systems in accordance with the Student Acceptable Use Agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:

Parents/carers play a crucial role in ensuring that their daughter/s understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website and on-line student records.
- their child's personal devices in the school

4. Education & Training

Staff:

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

- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events/ and or other relevant organisations.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required

Governors:

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation.
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons or online training).

7. Technical – infrastructure/equipment, filtering and monitoring:

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The school has provided enhanced user-level filtering
- Network Manager and senior staff monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any breach.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school.
- Users are not permitted to download and or install applications (including executable or similar types) on to a school device or whilst using the schools systems, without agreement from the IT department.
- Users may use the following types of removable media for the purposes detailed:
  - CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.

- USB Media (memory sticks) – this type of media can be used on school devices for transferring personal work. The use of applications on this type of media is strictly prohibited. All staff must use encrypted USB media. This is under review.
- Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

8. Data Protection and Security:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the schools' Data Protection Policy.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

The handling of protected school data is everyone's responsibility.

All staff must secure any personal data you hold about individuals and any data that is deemed sensitive or valuable.
The school has appointed a Senior Information Risk Owner (SIRO). This will be the Head teacher. The SIRO's has the following responsibilities

- They own the information risk policy and risk assessment
- They appoint the Information Asset Owners (IAOs)
- They act as an advocate for information risk management.

The school will appoint Information Asset Owner IAO.
The IAO must identify the information assets – including personal data for students and staff, assessment records, medical information and special educational needs data. The role of an IAO is to understand:

- What information is held, and for what purposes.
- How information has been amended or added to over time
- Who has access to protected data and why.

The IAO will likely to be TLCs, finance officer and Assistant Head.

Data is classified using the Government Protective Marking scheme to indicate sensitivity of data. All data, electronic or paper should be labelled according to the protection it requires, based on Impact Levels. This is currently under review.

Impact Level	Description
IL1	Not Protectively Marked
IL2	Protect
IL3	Restricted
IL4	Confidential

Not protectively marked - General teaching materials with no personal information.
Protected - Class lists including personal data, forenames, surnames.
Restricted - Student/staff CBDS (Common Basic Data Set) data held on MIS system or paper.
Confidential - Student /staff data containing very sensitive data e.g. drugs, counselling.

9. Data Transfer

Kendrick School recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

• Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location

• All emails that contain confidential information being sent outside of the school environment must be encrypted. Any document being sent must be encrypted and password protected. Password to be sent by a different method to email.

• Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school

• When restricted or protected personal data is required by an authorised user from outside the organisation's premises they must use the remote access to do work.

• If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location

• Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and

• Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.

10. Communication

A wide range of rapidly developing communications technologies has the potential to enhance learning.
When using communication technologies, the school considers the following as good practice:

• The official school email service may be regarded as safe and secure.

• Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to such communication.
• Any digital communication between staff and students or parents/carers must be professional in tone and content.
• Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
• Personal information should not be posted on the school/ website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity:
All schools have a duty of care to provide a safe learning environment for students and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:
• Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
• Clear reporting guidance, including responsibilities, procedures and sanctions.
• Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
  Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Appropriate and Inappropriate Use by Staff:

Staff members have access to the network so that they can obtain age-appropriate resources for their classes and create folders for saving and managing resources.
They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
All staff should receive a copy of the Internet and E-Safety Policy and a copy of the Acceptable Use Agreement, which they need to sign.
When remoting into school from home, the same Acceptable Use Agreement will apply.

In the Event of Inappropriate Use by Staff
If a member of staff is believed to misuse the internet or school IT system in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then a disciplinary procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

This section is about Staff Usage and Monitoring

1. Working Online and Email and social media

- All staff are responsible to keep systems up to date with security and virus patches.
- Only download files or programs from sources you trust and be wary of links to websites in emails, particularly from people you do not know.
- Report any spam or phishing emails that are not blocked to the IT team.
- Do not respond to emails asking you to confirm personal information such as passwords, bank details etc.
- Do not email any sensitive information (e.g., student details) unless you know it is encrypted by using Egress software.
- All Internet access for students and staff is monitored by Securley and any concerns are automatically reported to AWE and a member of SLT.
-

Any professional communications that utilise technology between the school and students, their families or external agencies should:
- take place within clear and explicit professional boundaries
- be transparent and open to scrutiny
- staff must not share any personal information with a student.

See code of conduct policy.

2. Passwords

- Use a strong password (8 characters or more including upper and lower case, plus numbers or character).
- Do not share passwords with other people.
- Do not use your work passwords for your own personal accounts.
- Do change your password regularly.
- Keep passwords secure.

3. General

- Shut laptops and computers down; do not hibernate whilst logged in.
- Use ctrl, Alt, Del to screen lock your computer if you walk away from it.
- Ideally keep laptops locked away when not in use.

- Keep personal data on the laptop to a minimum.
- Ensure your laptop is fully encrypted.
- When sending and sharing, be aware with whom you can share data with.
- Do not pass data to third parties without checking how they will secure it.
- Do not send student data or CTF's via email outside of the secure network.
- Do use the DFE S2S system to transfer data securely
- Do not use removable media, e.g. USB drives, CD etc. unless it is encrypted.
- Ensure data is only accessible by those people that need to have it.
- When working on or off site lock sensitive information away when left unattended (e.g. student/staff files).
- Do not let strangers in to staff or student areas.
- Ensure screens cannot be overlooked by anyone.
- Only take information offsite which you are authorised to have.
- Wherever possible access data remotely.
- Personal data sent over the Internet must be encrypted or otherwise secured;
- Encrypted USB storage devices must always be used if transfer data (if not being done by other more secure ways).
- All staff laptops must be encrypted.
- No student data must be stored on any home computer. Staff will need to remote in/ or use SharePoint and or Google Cloud services to access student information.

4. Staff Email Protocol

Email is used for communication at Kendrick between students/staff and stakeholders. This protocol is for us to manage our vast amount of email. Below are some basic guidelines.

1. A clear, direct subject line.
Always add a subject line to your emails so it is clear for what you want to communicate e.g., Confidential Safeguarding or Cover. Only include initials of students. It is helpful to put "Response needed" or "For info" at the start to indicate if a response is needed.
2. Think twice before hitting 'reply all.'
Consider who to reply to and refrain from hitting "reply all" unless everyone on the list needs to receive the email.
3. Use professional salutations.
Use Dear or Hello for internal emails. Sign off in a professional way.
4. Tone and humour
Emails at the workplace must have a formal tone to them. There is always a higher chance of miscommunication over emails because your words are not accompanied by gestures, body language and facial expressions. Be polite, choose your words wisely, use proper punctuation and avoid capitalizing all your words. Be careful with using exclamation mark.
Humour can easily get lost in translation without the right tone or facial expressions. It is better to leave humour out of emails.
5. Reply to your emails
If you receive an email from a parent reply within one working day.
6. Proofread every message.
Your mistakes will not go unnoticed by the recipients of your email. Do not rely on spell-checkers. Read your email before sending it off.
7. Double-check that you have selected the correct recipient.
Pay careful attention when typing a name from your address book on the email's "To" line.
8. Nothing is confidential.
Every electronic message leaves a trail. A basic guideline is to assume that others will see what you write. Do not write anything you would not want everyone to see.
9. Length of emails
Keep your emails short and to the point unless you need to have the information as a record such as a pastoral concern. Bullet points can be useful. Would it be better to have a conversation with the person than a long email?
10. Times Sending emails to students and staff
Emails should only be sent to students/staff between 7.00am -6.00pm within school working days. They should not be sent at weekends or in the holidays. Staff not to send emails after 6.00pm unless urgent. Type and put in your draft box or use delay function to send the following day.
11. Email management
Please delete unwanted emails.
12. Attachments
Use hyperlinks to documents rather than send an attachment.

This section is about Student Usage and Monitoring

1. Benefits to Students and the School

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between students world-wide
- vocational, social and leisure use in libraries, clubs and at home
- access to experts in many fields for students and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across networks of schools, support services and professional associations

- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data with DfE
- Access to learning wherever and whenever convenient

The purpose of Internet use in school is to:

- raise educational standards
- to promote student achievement
- to support the professional work of staff
- to enhance the school's management functions

Internet access is an entitlement for students who show a responsible and mature approach to its use.

2. How will the Internet support effective personalized learning?

The school commitment to personalised learning is clearly supported through its use of the internet and e-mail as learning tools. Encouragement and support is offered to students within specific subject areas and as IT as a whole. In encouraging independent use of the Internet, the school is aware that students may encounter sites which are inappropriate. It will prevent this whenever possible through the filtering system of the Internet Service Provider (ISP) and through encouragement of responsible use of the internet. A careful and sensible balance between the protection of students and a flexible independent learning tool must be maintained; both careful monitoring and trust in the students' maturity are important.

- Internet access for students and staff is filtered and monitored by the school via its ISP.
- All Internet access for studednts and staff is monitored by Securley and any concerns are automatically reported to AWE and Key Stage pastoral leaders.
- Internet access will be planned by teachers and encouraged to enrich and extend learning activities.
- Students will be given clear objectives for Internet use in the classroom and staff will select sites which will support the learning outcomes planned for students' age and maturity.
- Recommended sites can be book marked, listed or copied to the school SharePoint;
- If students do not follow objectives given by the member of staff in charge relating to internet use, disciplinarily action will be taken, referred to in later sections.
- Students will be educated in taking responsibility for Internet access. Responsible independent use of the internet will be encouraged through Computing lessons and through discussion of the "Acceptable Internet Use Statement", which is available for viewing on the SharePoint.
- Staff must regard copyright laws when using material from the internet – see copyright policy.

3. How will students be taught to assess Internet content?

- Students will be taught ways to validate information before accepting that it is necessarily true;
- Students will be taught to acknowledge the source of information and observe copyright when using Internet material for their own use;
- Students will be made aware that the writer of an e-mail or the author of a Web page might not be the person claimed;
- Students will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
- These teachings will occur in the first Computing class of every year, with higher years receiving a re-cap or update of the system and any changes made to it during the previous year. This ensures that all students are kept up to date and informed about the workings of the school computer system and the policies surrounding it.
- Students will be made aware of positive and negative digital footprints in the curriculum.

4. How will social networking, social media and personal publishing be managed?

- Students will be advised never to give out personal details of any kind which may identify them and /or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Students should be advised not to place personal photographs on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or her location.
- Staff official blogs or wikis should be run from the school domain with approval from the Senior Leadership Team. Staff should be advised not to run social network spaces for student use on a personal basis.
- If personal publishing is to be used with students, then it must use age-appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.
- Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- The school supports staff contacting students and parents via e-mail but line managers must be copied in when contacting parents. For school trips student contact numbers may be stored on a school mobile but must be deleted after the trip. Staff are not to use personal social networking sites for communicating with students.
- See Staff Code of Conduct Section 22 Social Media for more details.

5. How will Internet access be authorised?

- Internet access is a necessary part of statutory curriculum. It is an entitlement for students based on responsible use;
- Students and staff are given Internet access but must sign the Acceptable Use Policy (AUP).
- A record will be maintained of all those with Internet access. Staff and students will be removed from the system when access is no longer required or is withdrawn.

6. How will out of lesson Internet access be monitored?

- It is not feasible to supervise all use of Internet access outside of lesson time and therefore computer use cannot be monitored directly;
- The standard monitoring through Internet Logs and the filtering of sites through Securly, will remain in place at all times;
- Students are expected to use the Internet in an appropriate and responsible manner in accordance to the AUP.

7. How will the Internet access of mobile devices be monitored?

- Any personal mobile devices which are capable of Internet access, but not connected to the Kendrick network, would theoretically be able to access inappropriate material;
- As a result, parents are responsible for any inappropriate material accessed via these devices;
- However, any inappropriate usage which occurs during school hours on the school premises can be dealt with at the school's discretion, even if the material was not accessed via the Kendrick network.
- SLT have the authority to investigate the content of mobile phones and other devices if misuse of inappropriate material is being accessed.

8. How will the school ensure Internet and e-mail access is safe?

- All users will be informed that Internet use will be supervised and monitored. This will be achieved through the filtering of inappropriate internet usage and the logging of students' online activity
- The Assistant Head, Network manager and the E-safety governor are responsible for monitoring use of internet
- Access to Internet logs will be restricted to the Assistant Head, Network Manager, E-safety governor and the school leadership team (SLT) and Key Stage leaders (TLC team).
- The school reserves the right to bar access to any web site it considers inappropriate. During lessons what is regarded as appropriate is at the teacher's discretion
- The school will work in partnership with the DfE and the ISP to ensure systems to protect students are reviewed and improved
- Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are effective in practice
- Any material that the school suspects is illegal will be referred to the appropriate authorities (e.g. Headteacher, Chair of governors and police.
- If staff or sixth form students require non-filtered Internet access, separate facilities will be provided if a valid reason is supplied
- The school's ISP filtering system will limit access to public chat rooms
- The Acceptable Internet Use Policy will detail activities and uses of the internet and e-mail, which are forbidden

9. How will the risks be assessed?

- The school will take all reasonable precautions via its ISP to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a device connected to the school network;
- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990;
- Methods to identify, assess and minimise risks will be reviewed regularly by the Assistant Headteacher and IT Network Manager and E-safety governor.
- The Head teacher is responsible for ensuring that the policy is implemented.

10. How will incidents be handled?

- Responsibility for handling serious incidents will rest with the SLT;
- Parents and students will need to work in partnership with staff to resolve issues. Parents will be contacted if a serious incident arises.
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies;
- A student may have e-mail, Internet or computer access denied for a period of time depending on the nature of the incident;
- Denial of access could include all schoolwork held on the system, including any examination work.

11. Timetable of events

- There will be regular communications to each year group regarding e-safety
- Year 7 have lessons on e-safety and year 8-11 have a re-cap at the beginning of every year.
- The e-safety group will regularly review the e-safety document throughout the year.
- This document will be reviewed every two years.
- All staff and students will sign the AUP.

12. Student Email Protocol

Writing an email to your teachers:

1. Use a short, accurate subject line – use keywords that summarises your email content
2. Use a professional font – Calibri, Times New Roman, Arial (font size 11 or 12)
3. At the start of your email address your teacher appropriately and politely, using their surname e.g. Dear Ms Smith
4. At the end of your email, sign it off politely with your name and form e.g. Thank you or Many thanks, Cara Blanshard
5. Use formal language, avoid slang, emojis and use complete sentences and polite phrasing
6. Check for spelling and grammar.
7. Always double check you are sending it to the correct recipient
8. Always send using your Kendrick School email address
9. Always send at an appropriate time i.e., 7am-6pm (no late-night emails)
10. Be wary of 'reply all' when replying to emails sent to a group.

Artificial intelligence AI

AI use refers to the use of AI tools to obtain information and content which might be used in work produced for assessments which lead towards qualifications.

While the range of AI tools, and their capabilities, is likely to expand greatly in the near future, misuse of AI tools in relation to qualification assessments at any time constitutes malpractice. Teachers and students should also be aware that AI tools are still being developed and there are often limitations to their use, such as producing inaccurate or inappropriate content.

AI chatbots are AI tools which generate text in response to user prompts and questions. Users can ask follow-up questions or ask the chatbot to revise the responses already provided. AI chatbots respond to prompts based upon patterns in the data sets (large language model) upon which they have been trained. They generate responses which are statistically likely to be relevant and appropriate. AI chatbots can complete tasks such as the following:

- Answering questions
- Analysing, improving, and summarising text
- Authoring essays, articles, fiction, and non-fiction
- Writing computer code
- Translating text from one language to another
  Generating new ideas, prompts, or suggestions for a given topic or theme
- Generating text with specific attributes, such as tone, sentiment, or formality

AI chatbots currently available include:

- ChatGPT (https://chatgbt.net/chatgpt-login/)
- Jenni AI (https://jenni.ai)
- Jasper AI (https://www.jasper.ai/)
- Writesonic (https://writesonic.com/chat/)
- Bloomai (https://huggingface.co/bigscience/bloom)
    - Google Bard

There are also AI tools which can be used to generate images, such as:

- Midjourney (https://midjourney.com/showcase/top/)
- Stable Diffusion (https://stablediffusionweb.com/)
- Dalle-E 2 (OpenAI) (https://openai.com/dall-e-2/)

The use of AI chatbots may pose significant risks if used by students completing qualification assessments. As noted above, they have been developed to produce responses based upon the statistical likelihood of the language selected being an appropriate response and so the responses cannot be relied upon. AI chatbots often produce answers which may seem convincing but contain incorrect or biased information. Some AI chatbots have been identified as providing dangerous and harmful answers to questions and some can also produce fake references to books/ articles by real or fake people.

AI tools must only be used when the conditions of the assessment permit the use of the internet and where the student is able to demonstrate that the final submission is the product of their own independent work and independent thinking.

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

- Copying or paraphrasing sections of AI-generated content so that the work 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 tools when they have been used as a source of information
- Incomplete or poor acknowledgement of AI tools
- Submitting work with intentionally incomplete or misleading references or bibliographies.

In exam assessments, AI misuse constitutes malpractice. Staff must discuss the use of AI and agree their approach with students. Staff must make students aware of the appropriate and inappropriate use of AI, the risks of using AI, and the possible consequences of using AI inappropriately in a qualification assessment. They should also make students aware of the centre's approach to plagiarism and the consequences of malpractice.

Staff must explain the importance of students submitting their own independent work (a result of their own efforts, independent research, etc) for assessments.

It may be that staff want students to use AI for particular assignments but discussions about general use for other work is important.
It remains essential that students are clear about the importance of referencing the sources they have used when producing work for an assessment, and that they know how to do this. Appropriate referencing is a means of demonstrating academic integrity and is key to maintaining the integrity of assessments. If a student uses an AI tool which provides details of the sources it has used in generating content, these sources must be verified by the student and referenced in their work in the normal way. Where an AI tool does not provide such details, students should ensure that they independently verify the AI-generated content – and then reference the sources they have used.

In addition to the above, where students use AI, they must acknowledge its use and show clearly how they have used it. This allows staff to review how AI has been used. Where AI tools have been used as a source of information, a student's acknowledgement must show the name of the AI source used and should show the date the content was generated. For example: ChatGPT 3.5 (https://openai.com/ blog/chatgpt/), 25/01/2023.

Identifying the misuse of AI by students

Comparison with previous work

When reviewing a given piece of work to ensure its authenticity, it is useful to compare it against other work created by the student. Where the work is made up of writing, one can make note of the following characteristics:

- Spelling and punctuation
- Grammatical usage

- Writing style and tone
- Vocabulary
- Complexity and coherency
- General understanding and working level

- The mode of production (i.e., whether handwritten or word-processed)

Potential indicators of AI use

If you see the following in student work, it may be an indication that they have misused AI:

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

b) A default use of language or vocabulary which might not appropriate to the qualification level*

c) A lack of direct quotations and/or use of references where these are required/ expected~

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 might be notable for some subjects

f) Instances of incorrect/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 this

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 themself, 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

Automated detection

AI chatbots, as large language models, produce content by 'guessing' the most likely next word in a sequence. This means that AI-generated content uses the most common combinations of words, unlike humans who use a variety of words in their normal writing. Several programs and services use this difference to statistically analyse written content and determine the likelihood that it was produced by AI:

- OpenAI Classifier (https://openai.com/blog/new-ai-classifier-for-indicating-ai-written-text/)
- GPTZero (https://gptzero.me/)

- The Giant Language Model Test Room (GLTR) (http://gltr.io/dist/)

AI detection will shortly be added to the existing tool Turnitin Originality (https://www.turnitin.com/products/originality

This tool features an AI review of a student's work, reviewing a portfolio of evidence and, we understand, will indicate the likelihood of AI use.

13. Glossary

AUP – acceptable use policy
AI - artificial intelligence
DfE – Department of Education
ISP – Internet Service Provider
IAO – Information Asset Owner
CBDS – Common Basic Data Set
MIS – Management Information system
IM – instant messaging

Acceptable Internet and E-mail/data Use Policy Agreement
For Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system and monitors Internet sites visited.

- Access should only be made via the authorised account and password which should not be made available to any other person;
- Activity that threatens the integrity of the school IT systems, or that attacks or corrupts other systems, is forbidden;
- All Internet use should be appropriate to staff professional activity or to students' education; legitimate private interests may be followed, providing school use is not compromised;
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate accessed and should expect to have their access removed;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- For emails the same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded;
- Any professional communications that utilise technology between the school and students, their families or external agencies should: take place within clear and explicit professional boundaries, be transparent and open to scrutiny and not share any personal information with a student.
- Use of chat rooms, posting anonymous messages and forwarding chain letters is forbidden;
- Copyright of materials and intellectual property rights must be respected;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Encrypted USB storage device must be used.
- All staff laptops must be encrypted.
- Any laptop/ pc removed from the school site must be encrypted.
- No student data must be stored on any home computer. Staff must use remote access or use SharePoint to access student information.

I understand that this agreement will remain in force until I leave Kendrick School.

To be completed by Member of Staff

FullName...

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

Acceptable Use of Digital Technology Agreement for Students

The computer system is owned by the school and is made available to you to further your education. The school's Internet Access Policy has been drawn up to protect you.

You need to know that the school can examine any files that may be held on digital devices and will monitor Internet sites you visit.

1. No one should access your account and you should not tell anyone your password;
2. Any use of IT systems considered inappropriate is forbidden;
3. You must only access sites and materials appropriate for your school work;
4. If you receive inappropriate emails or texts you should tell your parents and Head of Year;
5. The language and content you use in emails, texts and social media should be appropriate i.e. no swearing or and offensive language;
6. You must not give out any personal information about yourselves, your friends or your family online including home address, phone or mobile number;
7. Use of chat rooms, posting anonymous messages and forwarding chain letters is forbidden;
8. Bullying is forbidden in all aspects of school life. IT and texting misuse will be seriously reprimanded and may forfeit use of the IT system;
9. You must respect copyright of materials and intellectual property rights;
10. Use for personal financial gain, gambling, political purposes or advertising is forbidden;

11. In Year 7 to Year 11 you are not allowed to be use mobile phones in school unless permission is given by a member of staff;
12. Always tell your parent or a teacher immediately if you come across anything you are unhappy with.
13. Use of AI is not allowed to complete assignments unless directed by our teacher otherwise.

By signing the “Acceptable Use of Digital Technology Agreement” you are indicating agreement with it.

I understand that this agreement will remain in force until I leave Kendrick School.

To be completed by Student

«Forename» «Surname» «Reg»

Signed by Student..

Signed by Parent/Carer..Date.............................