Friends' School Lisburn

E-Safety Policy

Contents:

At Friends' School Lisburn, we prioritise the safety and responsible use of digital and online technologies within our school community. By providing clear guidelines and procedures, we strive to ensure that technology enhances teaching and learning while keeping our students safe.

1. Aims:

Safe and Responsible Use:

- Promote the safe and responsible use of digital and online technologies in line with our school's values
- Enhance teaching and learning through the effective and secure use of ICT facilities

2. Roles and Responsibilities:

Governors:

- Approve and review the E-Safety Policy
- Provide guidance and support to the school community in e-safety matters

Principal and Leadership Team:

- Familiarise themselves with the procedures for handling serious e-safety allegations involving staff members
- Ensure appropriate training is provided to staff for their e-safety roles and responsibilities
- Will aim to be progressive about responses to changes Digital Technology brings to society. The Principal & Leadership team will risk-assess any new technologies before they are allowed in School, and will consider any educational benefits that they may have and will develop appropriate strategies for dealing with new technological developments and any associated risks

The Director of IT supported by the school IT technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed as required
- the school's filtering policy (currently determined by C2K), is reviewed regularly to take account of any new online threats or content deemed inappropriate or harmful
- stays 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 the use of the network, G-Suite and email is regularly

monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies
- Provide training and guidance to staff on e-safety matters
- Collaborate with technical staff to maintain a secure online environment
- Document and report e-safety incidents to inform future developments
- Regularly update the Leadership Team and Governors on e-safety issues

Designated Teachers for Safeguarding:
- Receive training on e-safety issues and child protection concerns
- Understand potential risks associated with
    - personal data sharing
    - illegal content access
    - inappropriate online contact
    - grooming
    - cyberbullying

Staff:
Teaching and non-teaching staff will:
- Contribute to the development of E-Safety Policies and procedures
- Receive training and guidance on e-safety matters and embed e-safety education in curriculum delivery where possible
- Act according to the Staff Acceptable Use of ICT Policy
- Report any concerns to the Designated Teacher for E-Safety

3. School Systems:
Managed System:
- The school utilises a Managed System maintained by C2k/Capita
- All equipment is maintained securely, and access is limited to authorised individuals
- Users are provided with secure usernames, generated by C2K, and passwords and are responsible for their security

School Managed Systems (Apple suites in Music & MIA)
- The school manages two non-C2K Apple-based networks (Art & Music departments)
- Internet access is provided wireless through the C2K Wireless network and as such the C2K filtering policy applies to all Internet traffic from machines in both the Art and Music IT suites
- All equipment should be maintained securely, and access limited only to students when under teacher supervision
- Students using machines in these spaces are provided with secure usernames and passwords on a workstation-by-workstation basis
- It is the responsibility of students using these devices to ensure they back-up any critical files/folders to protect against data loss. Neither networks currently have network backup facilities (under review) and files are stored locally on the device

Internet Filtering and Services:
- Implement differentiated filtering levels to ensure safe internet access for different user groups
- Promote the use of C2k services, including C2k email and the G-Suite which includes Google Classroom, Google Drive and Google Sites to provide all virtual learning services

Personal Use and Removable Media:
- Establish clear policies regarding personal use on school systems and devices outside of school (refer to Appendix 3)
- Develop policies addressing the use of removable media (refer to Appendix 2)

Data Protection:

- Prohibit the transmission of personal data over the internet or off-site without proper encryption or security measures
- Refer to the Data Protection Policy (GDPR - Appendix 4) for detailed guidelines

4. Pupils:

E-Safety Education:

- Provide specific guidance on safe and acceptable online behaviour through ICT classes during timetabled class in Years 8 and 9, anti-bullying initiatives, and Personal Development units as part of the Key Stage 3 LLW curriculum
- Reinforce key e-safety messages through assemblies, pastoral activities, external agency involvement (e.g., PSNI), and School Planner references
- Integrate e-safety content into curriculum schemes of work across all subjects

Bring Your Own Device (BYOD):

- Students in Years 8-14 are allowed to use their own personal devices in the classroom subject to the approval of the classroom teacher concerned. Sixth Form pupils may also use their personal devices in Private Study to aid their studies and are subject to the requirements as laid out in the Acceptable Use Policy (see Appendix 2). Students must also use the "C2K Wireless" Wi-Fi network to connect to the internet to ensure all websites etc. are filtered according to the prevailing C2K web filtering policy. Personal devices can only be used after pupils have read and signed the Pupil acceptable use policy (Appendix 1)

5. Cyberbullying:

- Prohibit the posting of offensive material related to the school, staff members, or students
- Strictly forbid all forms of cyberbullying, addressing incidents in line with the school's Anti-Bullying Policy
- Encourage students to report instances of online bullying to staff members promptly
- If staff feel that they are abused online, they should speak to a member of SLT as soon as possible

6. Staff:

- Encourage staff members to be positive role models in their use of digital technologies, the internet, and mobile devices
- Provide annual e-safety training as part of safeguarding training
- Include e-safety in the Continuous Professional Development (CPD) program for all staff

7. Parents:

- Educate parents and carers on the importance of responsible internet and mobile device use
- Share e-safety information through School Planners, InTouch, and organised talks
- Encourage parents to support the school's efforts in promoting good e-safety practices

8. Use of Digital and Video Images:

- Raise awareness among staff, parents, and pupils about the risks associated with publishing digital images on the internet
- Obtain written permission from parents for image use for publicity purposes
- Specify guidelines for staff and volunteers regarding the use and publication of digital and video images
- Promote responsible behaviour and respect for privacy when capturing or sharing images
- Comply with good practice guidance for selecting and publishing photographs and pupil work on the school website or other platforms
- The Bursar is responsible for the operation of CCTV which is used to monitor certain areas of the school premises. Appropriate signage indicates the presence of CCTV cameras at all locations and no additional cameras should be installed by anyone anywhere on the school premises. Images taken by CCTV cameras are stored and may be reviewed if necessary

9. Artificial Intelligence (AI):

- Raise awareness among staff, parents and pupils of the benefits and risks associated with AI
- Specify guidelines for staff and pupils with the use of AI in education
- Promote responsible and JCQ compliant use of AI

10. Infringements of the E-Safety Policy:

- Address incidents of careless, irresponsible, or deliberate misuse of school systems or devices promptly and proportionately
- Keep clear records of investigations and follow established school policies, including the Anti-Bullying Policy
- Report suspected illegal activities involving school systems or devices to the appropriate authorities
- In the case of more serious infringements, the following procedure will be followed:
    - *a designated computer not used by young people will be used*
    - *sites and content visited will be closely monitored and recorded*
    - *URLs and screenshots may be recorded for investigation, except in the case of images of child sexual abuse, where the matter will be referred immediately to the police*
    - *the computer in question will be isolated, as any change to its state may hinder a later police investigation*
    - *clear records will be kept of the investigation*

If there is reason to believe that illegal activity has occurred using school systems or school devices, the matter will be passed on to the police.

Appendix 1: Friends' School Lisburn
Acceptable Use of ICT Policy for Pupils

This AUP should be read in the broader context of the School E-Safety Policy and has two main aims:
1. to enhance learning by allowing pupils at Friends' the freedom to use School ICT facilities and individually owned mobile electronic devices as a tool to help them in their learning.
2. to protect the school community from the negative aspects of the use of ICT.

C2k Managed Service

A filtered internet and email service is provided in School through C2k. All pupils are provided with an email address and password. Pupils are encouraged to use this facility to:

- research, create, store and print material related to the curriculum
- communicate with other pupils, members of staff, recognised outside agencies and pupils in partner schools
- support their learning through Virtual Learning Environments, such as Google Classroom

Pupils should know and understand that no user of School services is permitted to:

- use another user's password or user name
- introduce unauthorised software to the system
- cause damage to equipment

Pupils are advised that School has the ability to review files and communications, and to monitor work remotely, to ensure that everyone is using the system responsibly.

In addition to using ICT facilities in classrooms, pupils may bring their own mobile electronic devices into School to help them with their learning, either in class or in Private Study. It should be noted, however, that no pupil should feel obliged to bring a device into school. If a pupil wishes to use their own mobile electronic device in school they should sign the declaration at the end of this Acceptable Use Policy. The school accepts no liability in respect of any loss/damage to personal ICT devices while at school or during school activities. The decision to bring a personal ICT device into school rests with the student and their parent(s)/guardian(s), as does the liability for any loss/damage. For the purposes of this policy, the term 'mobile electronic devices' includes mobile phones, laptops, netbooks, tablet computers, mp3 players and other similar devices capable of storing information and sending and receiving data via the internet. Most of these devices also have the capacity to record both sound and still and moving images.

Use of the internet
Access to the internet in school should be exclusively through the C2k network. Pupils when using their devices should only use the C2k WiFi service. It is School policy to promote the use of C2k services, including C2k email and Google Classroom. Pupils should not use the mobile phone network to access the internet unless they have permission from a member of staff to do so. Pupils using devices with internet capability should be aware that downloading data may incur a cost.

The following online activities are not permitted:

- the use of social networking, file sharing or gaming sites, unless permission has been given by a member of staff in relation to a classroom activity
- unfair usage (for example, downloading or uploading large files, or using streaming services such as Netflix, Disney+ and Amazon Prime, which hinders others in their use of the internet for educational purposes)

Recording and storage of sound and images
The recording and storage of sound, or of still or moving images is allowed only with the permission of a member of staff. If images are recorded, this will be done in accordance with the School's policy on the use of photography.

Photographs, sound files or videos produced in School should not be posted on the internet unless there are special circumstances in which permission to do so has been granted. Pupils must allow staff access to images and sound files created in school, including those stored on personally owned electronic devices, and must delete them if requested to do so.

Cyberbullying

Offensive material relating to School, members of staff or other pupils should not be posted on the internet, regardless of whether this has been done at school or in any other place, including a pupil's home.

All instances of cyberbullying – online behaviour which seeks to harass, intimidate or humiliate others – is strictly forbidden and will be dealt with in line with the school's Anti-Bullying policy. If pupils think they are being bullied online, they should speak to a member of staff as soon as possible.

Social Media

Pupils should ensure that:

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not attributed to the school
- Security settings on personal social media profiles are regularly checked

Artificial Intelligence (AI):

AI or artificial intelligence in education refers to the use of AI tools to obtain information and content which might be used in academic work.

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

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.

Pupils should:

- Be mindful of the benefits and problems of using AI tools and endeavour to stay within AI Guardrails as established within school (see below)
- Only use AI (whether at home or in school) to produce academic work with the express permission of a member of staff
- Be aware that they are NOT allowed to use AI tools when in an exam
- Be aware that at GCSE, AS and A2 Level the rules regarding the use of AI are specified by JCQ. The rules will depend upon the qualification followed and pupils must check with their teachers to what extent AI tools may be used in the production of academic work
- Reference their use of AI tools if they are allowed to use it in the production of academic work. This will include the name of the AI tool the pupil used, the date the pupil generated the content, include an explanation of how it has been used and save a screenshot of the questions asked and responses given
- Be aware that if AI has been used in the production of work that is used in the assessment that contributes to a qualification, that a declaration must be signed after appropriate referencing has occurred. Failure to follow procedures may be deemed to be malpractice which may result in the loss of marks or disqualification from a subject

FSL GUARDRAILS

Educational Impact

AI can be **a teaching and learning tool**

Teacher relationship, expertise and management are the key to the learning process

It is best used for a **focused and designated pedagogical benefit**

Consider overreliance on AI or technology

Ethical Compliance

Consider ethical and legal uses of AI

Where do AI generated results come from?

Is it accurate or biased?

How do you know?

Academic Compliance

Respect intellectual property

Promote accurate representations of pupil ability

Reference relevent work

Data Security

Consider and protect the privacy and data of all stakeholders

No personal or indentifiable data should be given to AI

Alert users when AI is being used and **explain how/what data is being held**

Human Involvement

AI should enhance not replace human interaction and creativity

AI can reduce the admin workload of staff but only effectively with human input

Take steps to verify the suitability, accuracy, and relevance of any AI-generated materials

Safeguarding

Users must be at least 13 years old due to potential AI misuse

Beware of **reliability, deepfakes,** and potential **impersonation**

Additional notes on the use of mobile electronic devices

Use of electronic devices in class is entirely at the discretion of teaching staff. Pupils should follow the instructions of their teachers and should not access any websites, apps or programs other than those required for the completion of the task set. Pupils who wish to use a device in school are required to sign this Acceptable Use Policy. With the variety of devices and operating systems pupils should be aware that no technical support will be offered with device-related issues connecting to the network. Only issues pertaining to C2K login will be supported by the school.

In accordance with the regulations set down by external Examination Boards, mobile telephones and other electronic devices such as memory pens, cameras and watches which can send, receive or store data are expressly prohibited in examination rooms. In addition, pupils are not permitted to have mobile electronic devices in examination rooms during internal examinations.

When not in use in class or in Private Study, electronic devices, including mobile phones, should not be switched on, except with the permission of a member of staff, and they should be put away safely from 8.30am until the end of the school day (normally 3.30pm). The only exception is the Year 14 Common Room. If a pupil needs to contact home during School hours, a school telephone may be used, or pupils may ask a member of staff if they may use their device to contact home. If a parent needs to contact a pupil, the School Office can be telephoned and a message will be relayed promptly.

Pupils are responsible for the safekeeping of their mobile electronic devices. These should be password protected and pupils are advised to install electronic tracking software, as well as ensuring that their devices are adequately insured. The School does not accept responsibility for the theft or loss of devices, or damage to them. Pupils are also responsible for all software and applications installed on personal electronic devices. The School cannot accept any responsibility for problems associated with software and apps pupils installed on devices. Pupils should ensure that their devices are properly protected by suitable anti-virus software at all times.

Sanctions

If a pupil is found to be in breach of any aspect of this protocol, the School reserves the right to confiscate a pupil's electronic device, or to withdraw permission, either temporarily or permanently, for the pupil to bring the device into School. Should a device be confiscated, it will be stored safely and may then be collected by arrangement between the pupil and the member of staff at the end of the school day. Additional action may be taken in line with existing policies on Anti-Bullying and Behaviour for Learning.

If there are reasonable grounds to believe that a pupil's electronic device contains images, text messages or other material that may constitute evidence of criminal activity, the School reserves the right to pass devices on to the police for further investigation.

Revised March 2024

Pupils' Acceptable Use of ICT Policy - Declaration

I understand that the use of the Internet and electronic communication is granted to me as a privilege, in return for my acceptance of the agreement. Any misuse on my part may result in loss of privilege and other sanctions being taken. This also applies to any activity undertaken outside school which contravenes the Acceptable Use rules.
All online activity will be appropriate to:

- Ensure the safety and security of the school system
- Ensure respect for all members of the community
- Maintain the reputation of Friends' School

In particular this means:

- I will only access the school ICT system and Internet via my authorised account and password which I will not make available to others
- I will ensure that I do not wilfully damage the system or the work of other members of the school community by means of editing, copying or deleting work, malicious code (e.g. malware or virus infection), hacking or physical tampering
- I will use the internet responsibly and will only visit sites / use materials or programmes appropriate to my school studies
- I will not give my home address, phone number, send photos or videos or give any other personal information that could be used to identify me, my family or friends unless a trusted adult has given me permission
- I will never meet, or arrange a meeting, with someone I have only ever previously met online (e.g. through social media, email or the internet) unless I take a trusted adult with me
- If I receive any inappropriate material, I shall not respond and will immediately inform a member of staff
- I will not send or forward messages, publish or create material which is offensive, hurtful or otherwise upsetting to another person. I will not post anonymous messages
- Language which I use in electronic communication will be appropriate and suitable, as for all school work.
- I will not use mobile phones or any other electronic devices to take, publish or share pictures / videos of anyone without their permission
- I will respect copyright of all materials
- I will only use AI in the production of academic school work as directed by my teacher

In addition, I understand:

- Use of the network to knowingly access inappropriate materials (such as but not limited to materials which are pornographic, racist or offensive) is forbidden and may constitute a criminal offence
- Guidelines for the safe use of the Internet will be followed and I will report any materials / conduct which I fell is unacceptable
- School reserves the right to examine or delete any files that may be held on its computer system, to monitor any Internet sites visited and emails exchanged and if necessary to report anything which may constitute a criminal offence

Signed _____

Bring Your Own Device (BYOD) User Agreement - Pupil Declaration

- I request permission to use my own personal ICT device in school
- I have read and understood the e-Safety and the Acceptable Use of ICT Policy. I agree to be bound by all guidelines, rules and regulations contained within these policies
- I agree to use the device for educational use only
- I agree to connect to the school-based C2K wireless or networking services only while using my personal ICT device in school. I understand that connection to non-school provided wireless/networking services in school is prohibited
- I understand that I am solely responsible for the correct care, safety and security of my personal ICT device when in school

Pupil Name _____

Disclaimer - The school accepts no liability in respect of any loss/damage to personal ICT devices while at school or during school activities. The decision to bring a personal ICT device into school rests with the student and their parent(s)/guardian(s), as does the liability for any loss/damage.

It is a condition of agreeing to allow students to bring personal ICT devices into school, that the parent/guardian countersigning the permission slip accepts this disclaimer. I have read and understood the e-Safety and the Acceptable Use of ICT Policy and give my son/daughter approval to use a personal ICT device in school. I understand my son/daughter is personally and solely responsible for the correct care, safety and security of the device. I understand that the school accepts no liability in respect of any personal ICT device used in school by a student. I understand and accept the disclaimer. This contract will remain in force throughout my son's/daughter's time at school and may be revised to take account of technological advancements in the interests of pupil and staff safety.

Parent/Guardian Approval _____

Appendix 2: Friends' School Lisburn
Acceptable Use of ICT Policy for Staff

E-Safety

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 this Acceptable Use Policy
- they report any suspected misuse or problem
- all digital communications with pupils and parents are on a professional level and are only carried out using official school systems

In addition, all staff share responsibility for ensuring that:

- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- pupils are aware of their 'digital footprint' and how this can affect them
- they monitor the use of digital technologies and mobile devices, including phones, tablets, MP3 players and cameras, in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- settings on computers and mobile devices are secure so that no sensitive or personal information, including passwords and emails, are displayed on screens in classrooms
- particular care will also be taken while projecting information from a digital media device onto a whiteboard or other form of facility, as inappropriate material may be displayed

Communications

When using communication technologies the school considers the following as good practice:

- The official C2k email and Google Classroom services should be used where possible as it be regarded as safe and secure, and is monitored
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, or is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and pupils or parents must be professional in tone and content.
- Staff should respond to email correspondence from parents via the School office
- Pupils 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

School staff should ensure that:

- Due care is taken when reference is made on social media to pupils, parents or colleagues
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not attributed to the school
- Security settings on personal social media profiles are regularly checked

Digital Images

- Staff and volunteers may take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Images should not be stored any longer than is necessary on personally owned devices
- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

Mobile electronic devices (including mobile phones)

- Staff should not send texts or make private phone calls during class time
- Personal calls and texts should not be received in class time except in exceptional circumstances
- Staff are asked to use their discretion when using mobile devices on the school premises
- Digital images should not be stored on personal mobile devices
- Communication with pupils and parents should be restricted to School business, and staff are advised to use school telephones, C2k email or SIMS InTouch to communicate with pupils and parents
- Staff who have been issued with mobile electronic devices by School (including iPads) should ensure that these are used primarily for School purposes, and that access to them is restricted so that confidential information is not viewed by others
- School reserves the right to recall and redeploy devices in order to maximise the benefit of these devices in teaching and learning

Appropriate use of ICT

Staff are encouraged to use ICT to enhance teaching and learning and it is recognised that it can be useful in many different contexts, including on school trips and at events organised by School.
However, in the interests of their own safety and that of others, all staff should be aware of what constitutes appropriate professional conduct in matters relating to e-safety.

Care should be taken when using sites dedicated to online shopping, online gaming, file sharing and social media. In addition, the following activities are deemed unacceptable and may in some cases constitute illegal behaviour. They should not therefore be carried out in school or using school owned devices:

- Unfair usage (for example, downloading or uploading large files, thereby hindering others in their use of the internet)
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Using school systems or devices to run a private business
- Infringing copyright
- The publication of information which may be offensive to colleagues or breaches the integrity of the ethos of the school, or brings the school into disrepute
- Promotion of any kind of discrimination
- Threatening behaviour
- Creating or propagating computer viruses or other harmful files
- Holding or transferring data without a legitimate reason
- On-line gambling
- Viewing or distributing inappropriate content

Artificial Intelligence (AI):

AI or artificial intelligence in education refers to the use of AI tools to obtain information and content which might be used in academic work.
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

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.

Staff should:

- Know the schools approach to managing AI as outlined in the FSL Guardrails (See below). Staff are encouraged to investigate how this tool can aid their classroom teaching and learning process
- Familiarise themselves with the JCQ AI Use in Assessments guidance
- Plan how to prevent AI misuse in assessments by methods such as getting pupils to produce work in the classroom and discuss with pupils their understanding on an ongoing basis
- Communicate the approach to students and parents. Be clear with pupils when AI can and cannot be used, make sure pupils know how to reference clearly and remind pupils of the importance of following exam guidelines / declarations
- Only accept work they consider to be the pupils' own. If a member of staff suspects AI has been used they should report this to HoY / HoD. If it is material that is part of work to be submitted to an awarding body it should be reported initially to a member of SLT

FSL GUARDRAILS

Educational Impact

AI can be **a teaching and learning tool**

Teacher relationship, expertise and management are the key to the learning process

It is best used for a **focused and designated pedagogical benefit**

Consider overreliance on AI or technology

Ethical Compliance

Consider ethical and legal uses of AI

Where do AI generated results come from?

Is it accurate or biased?

How do you know?

Academic Compliance

Respect intellectual property

Promote accurate representations of pupil ability

Reference relevent work

Data Security

Consider and protect the privacy and data of all stakeholders

No personal or indentifiable data should be given to AI

Alert users when AI is being used and **explain how/what data is being held**

Human Involvement

AI should enhance not replace human interaction and creativity

AI can reduce the admin workload of staff but only effectively with human input

Take steps to verify the suitability, accuracy, and relevance of any AI-generated materials

Safeguarding

Users must be at least 13 years old due to potential AI misuse

Beware of **reliability, deepfakes,** and potential **impersonation**

STAFF GUIDANCE ON REMOTE PARENT TEACHER MEETINGS

Introduction

The School acknowledges the value of online platforms in enabling Parent Teacher Consultations to take place remotely. The main platform for this is School Cloud. Online consultations will have been organised by a Senior Teacher and Head of Departments are responsible for ensuring that appropriate staffing arrangements / requirements are in place prior to the Parent Teacher Consultation. Online consultation is an extension of the classroom and is covered by this e-Safety, Acceptable Use Policy & Behaviour Policy. All principles outlined by these policies will also apply.

(a) **Security**

- Staff should only use the provided online platform for Parent Teacher Consultation
- Particular care should also be taken while sharing information (screen sharing) as inappropriate material may be displayed
- Any suspicious online activity must be reported immediately to a member of the Safeguarding Team

(b) **Location, Appearance and Behaviour**

- When engaged in live-streams, Staff should ensure that their location has no sensitive images or materials visible which could be transmitted from their web cam
- Staff should be aware that all normal professional teaching standards apply for instance the choice of camera location and use of professional language and conduct

(c) **Protocol**

- There should be a minimum of two adult participants (one teacher and at least one parent) in an Online Parent Consultation
- Pupils are not permitted to engage in a remote parent teacher consultation without a parent present

(d) **Reporting Concerns**

- Safeguarding concerns should be reported immediately to the Designated or Deputy Designated Teachers
- Behavioural matters should be reported immediately to the relevant Head of Year

Staff iPad Protocol

The following are the conditions under which you accept the provision of the iPad. This Agreement will start on receipt of the iPad. These devices remain the property of the School at all times and are issued to staff for use in relation to their professional duties. Initially, there will be focus on how this device can be used as a tool to aid learning and teaching, including the effective assessment of pupil work. It will also be used as an administrative tool to facilitate staff meetings and meetings with parents.

A. Under the terms of this agreement, Friends' School Lisburn will:

1. Provide an iPad for use whilst a member of teaching staff at the school. As personal information may be contained on the iPad, it should not be used by any person who does not work in Friends' School
2. Set up the iPad, initially, to enable you to connect to and make effective use of the school network, software and hardware;
3. Plan and manage the effective use of iPads in school, and provide the professional development required to enable staff to use the iPad as a tool to enhance learning and teaching
4. Provide a **Mobile Device Management App** which will manage the installation of new software and associated updates. This app also allows the Director of ICT / ICT Technician to remotely trace and monitor the device if it is lost or stolen. The ability to trace and monitor the device will only be initiated if a device is reported as lost or stolen;
5. Provide a process for the installation of new software to the iPad. (No cost software applications should be made with the Director of ICT. Software applications that have an initial or ongoing subscription cost should be made with the Bursar)
6. Provide technical / maintenance support with the ICT Technician for the duration of the iPad's life span;
7. Provide insurance cover for the iPad
8. Have an expectation that staff will abide by the School's Acceptable Use Policy
9. Reserve the right to request the return / transfer the iPad at any time

B. With this agreement members of staff at Friends' School Lisburn will:

1. Use the iPad for the purposes for which it was provided, and at all times abide by the Acceptable Use Policy
2. Take part in training and participate fully in work on priorities identified in the School Development Plan
3. Return the iPad to the School on commencement of an extended period of leave or on leaving the teaching staff at Friends' School Lisburn
4. Return the device when requested to allow maintenance, updates and new software to be installed
5. Inform the ICT technician of any faults as soon as possible. Under no circumstances should anyone, other than the ICT Staff, attempt to repair suspected faults
6. Provide suitable care and security for the iPad at all times. All staff must use a passcode to access the iPad. If the iPad is lost, stolen, or damaged, the Bursar must be notified immediately
7. Follow the School processes to request for software applications to be installed on the iPad

Follow School advice on the configuration, network access and set up of the device. This will be subject to change as the technology, hardware and software develops.