ICT E-Safety & Acceptable Use Policy
for Students

This policy was adopted and reviewed by the Governing Body RIG Committee on 22nd January 2024.

This policy will be reviewed annually.

MISSION STATEMENT

At Grays Convent we recognise the value of each individual as a gift from God to the world. We are a Catholic school founded by the La Sainte Union Sisters and our ethos is one of unity, prayer, worship, service and work. We strive to follow the example of the Sacred Hearts of Jesus and Mary by enabling learning to take place in a caring and accepting community. We are blessed by Jesus the Good Shepherd, try to follow him in everything that we do, and in doing so make the most of our God given talents. We are one with God.

Introduction

The aim of this policy is to ensure that all members of Grays Convent School and in particular students benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner and to become prepared for the use of ICT systems in the world of work.

WHEN USING GRAYS CONVENT HIGH SCHOOL ICT EQUIPMENT THERE SHOULD BE NO EXPECTATION OF PRIVACY.

Internet use and access is considered a school resource. By accessing the internet using school facilities, students are agreeing to comply with the school rules for internet use. Therefore, if the school policy is not adhered to this privilege will be withdrawn and appropriate sanctions outlined in this policy will be imposed. All students sign an acceptable use policy in compliance with Child Exploitation and Online Protection (COEP) recommendations.

You should read the policy regulations and guidelines carefully to ensure that the content is accepted and understood.

2.   Definition of Unsuitable, Inappropriate and Unacceptable Use

Unsuitable – DO NOT send, download, display print or distribute material that is:-

- Sexually explicit
- Obscene
- Likely to cause complaints of sexual or racial harassment or bullying or any other form of harassment
- Intimidating
- Fraudulent or break copyright laws
- Defamatory
- Otherwise harmful
- Used to denigrate other people or organisations

Inappropriate –

The following uses of the Internet are specifically prohibited and will be dealt with as serious breaches of discipline:-

- Accessing web pages by writing in the numerical IP address
- Accessing any web page in order to download or play games, or to access 'Virals'
- Using Messenger or any other form of network based instant messaging service
- Accessing any chat room websites, instant messaging services, social networking sites (e.g. Facebook,) or Skype
- No files may be intentionally downloaded unless directed by staff. No programs may be introduced, nor installations made
- Downloading and/or distributing music files are not permitted except where you have been specifically told to do so by a staff member, it is part of your school work and all copyright conditions have been met
- Accounts must not be set up. Goods or services must not be ordered. Pay to view or chargeable services must not be accessed
- Accessing any website that contains the functionality to facilitate the bypassing of the school proxy server.

Disciplinary action may result if anyone is found to be involved in such activities.

Unacceptable Use -

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

> Using the school's ICT facilities to breach intellectual property rights or copyright

> Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination

> Breaching the school's policies or procedures

> Any illegal conduct, or statements which are deemed to be advocating illegal activity

> Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

> Activity which defames or disparages the school, or risks bringing the school into disrepute

> Sharing confidential information about the school, its pupils, or other members of the school community

> Connecting any device to the school's ICT network without approval from authorised personnel

> Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data

> Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

> Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

> Causing intentional damage to ICT facilities

> Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel

> Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

> Using inappropriate or offensive language

> Promoting a private business, unless that business is directly related to the school

> Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

> Using ICT or the internet to breach intellectual property rights or copyright

> Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination

> Breaching the school's policies or procedures

> Any illegal conduct, or statements which are deemed to be advocating illegal activity

> Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

> Activity which defames or disparages the school / school staff, or risks bringing the school into disrepute

> Sharing confidential information about the school, other pupils, or other members of the school community

> Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel

> Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

> Causing intentional damage to ICT facilities or materials

> Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

> Using inappropriate or offensive language

3.   Regulations & Guidelines

The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with ICT and the Internet. These strategies are as follows:

3.1   Internet

The Internet provides access to information on a wide variety of topics.

All Internet users in Grays Convent High School

- Will not be permitted to visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable material
- Must report any material of the above nature to a teacher/supervisor/Assistant/Deputy Headteacher or the Headteacher
- Will use the Internet for educational purposes only
- Will not upload, download or otherwise transmit material that is copyrighted
- Will not disclose or publicise personal or confidential information, for example their name or classmates' home addresses, telephone numbers, name and location of their school
- Will not examine, change or use another person's files, user name or password
- Will be aware that any computer usage, including distributing or receiving any information, school-related or personal, may be monitored for unusual activity, security, and/or network management reasons
- All Internet use is logged and access to many web sites will automatically be barred (either by our ISP or internally using the Grays Convent High School proxy server). Grays Convent does not expect its students to visit any inappropriate sites. If students become aware of inappropriate sites accessible, it is their responsibility to inform the teacher/supervisor/ICT support team
- The school outsources its broadband provision to London Grid for Learning. They provide filter and blocking and anti-virus services. The network manager regularly checks all safeguarding measures provided by LGfL. The school also blocks new sites deemed to be unsuitable including all social networking sites.
- Pupils should not use their mobile phones in school to access the internet unless it is for educational purposes and they are instructed to do so by a teacher. E.g. Use of Google Translate or an educational app.

3.1.1. School Website and Virtual Learning Environment (Google Classroom)

- The copyright of all material produced by the school for display on the school's web pages/Google Classroom belongs to the school. Permission to reproduce any other

material will be sought and obtained, from the copyright owner. Please seek permission through the Headteacher

- The publication of student work will be checked and validated by a teacher
- No pictures of any pupil will be added unless a parental consent form has been signed. Any picture added will follow CEOP guidelines.
- The school website has a CEOPs 'report it' button and the school takes part in the Safer Internet Campaign

3.2   E-mail

Grays Convent High School encourages staff and students to send emails instead of letters, faxes and other forms of paper communication where deemed appropriate (i.e. for school related communication). This form of contact provides quicker communication and also a convenient way of filing such documents. E-mail accounts will be supplied to all computer users. Please be aware that the system is automatically checked to protect against viruses, identifying the access of unsuitable material and for highlighting other illegal or inappropriate behaviour. Disciplinary action may result if anyone is found to be involved in such activities.

Students will use only approved email accounts under supervision or permission of a teacher.

Students will not arrange to meet someone outside school via email, the Internet or social networking sites. Pupils will note that sending and receiving email attachments is subject to permission from their teacher.

The school uses its own e-mail system which is Microsoft Outlook Exchange. Additional filters are in place to prevent spamming.

Students:

- Will not send or download any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person
- Will refrain from sending on chain e-mails
- Will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures
- Will not send unsolicited email to other students or teachers
- A student of the school who receives unsolicited email must immediately notify the sender that such e-mails are not permitted, must not be sent in the future and will be deleted unread and must notify a teacher or member of staff
- The school email system will not be used for any form of harassment
- Users of the school e-mail system will manage the size of their mail folder in accordance with the system-wide tier limits imposed. These are subject to change.

3.3   Social Networking, Instant Messaging & Chat Rooms

- Pupils must not use social networking sites, chat rooms, forums or blogs to post inappropriate, false or derogatory comments about other students, members of staff or the school as these sites are accessible by members of the public. Any instances where this occurs as a result of comments posted while out of school will result in disciplinary action. Access has been blocked to all social networking sites on the school network.
- Students Personal Use of Social Media :
  Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources.
- Any concerns regarding students use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Students will be advised:
- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.
- Pupils will only have access to discussion forums such as those found on the educational websites and the Grays Convent Google Classroom.
- Externally moderated chat rooms, discussion forums and newsgroups will be used only for educational purposes as directed by a teacher or member of staff
- Face to face meetings with someone organised via Internet chat will be forbidden
- All other forms of internet based Instant Messaging are prohibited, for example, Facebook, MSN Messenger, AOL IM and Yahoo IM.Skype
- Use of webcams in school is prohibited without teacher supervision.

3.4   School Infrastructure

3.4.1   Files and Directories

- Keep file and directory names meaningful, you may know what the contents are now but may forget in the future
- Keep all files on the server; the server is backed up every night. If you keep files on your local drive then this will be your responsibility
- Regularly perform housekeeping on your files and directories, delete unwanted files and check that the files are in the correct directory

- Try and create a hierarchy for your directories; it is far better to have ten directories with ten files each rather than one with a hundred
- USB Memory Sticks may not be used by pupils. Files can be transferred between home and school using either school email or Google Classroom. Everyone will have a personal directory. Although under normal circumstances the Network Manager will not access these directories users must be aware that Grays Convent High School reserves the right to review what is in these directories for security and legal reasons. Files brought in from home must not include programs or file types that are mentioned as forbidden in this policy.
- MP3, MP4, WMA and other compressed media file formats are not allowed to be stored on Grays Convent High School owned ICT resources unless authorised by a member of staff for educational purposes
- Password protected 'zip' files are not to be used; any found on the system will be deleted

3.4.2 Usernames, Passwords and Security

- You will be issued a username and password for email/VLE facilities. This is to be kept very secure
- Do not give your password to anyone else. If you do and that person does something that they shouldn't when logged in as you, you are responsible, as you should have not given your password to them
- Passwords will be required to access all ICT facilities in Grays Convent High School
- Passwords should be changed if there are fears that others may know them
- If you suspect other persons have your password then please inform the school's Network Manager
- We respect pupils' privacy; however, it is necessary for ICT staff to retain a list of pupil passwords for the curriculum network
- You will only have access to information on the server that has been deemed appropriate to you. If you think you need other information the Network Manager will discuss this with you
- Report any suspected security violations or weaknesses
- If you are temporarily leaving your workstation you must log off
- Use of another person's account, or allowing another person to use your account, to access any information/data is wholly unacceptable and will be dealt with as a breach of the Data Protection Act: this could result in police involvement and disciplinary action which may involve external agencies.

3.4.3 Unauthorised Software

- No unauthorised software can be loaded as students do not have administrative rights. Do NOT bring games, screen savers etc in and try to load them
- If you require anything in addition to what is pre-loaded then contact the Network Manager

3.4.4 Viruses

- ***A virus shield and suitable filters are provided by our ISP with is London Grid for Learning.*** Although this provides protection, please be on guard for any suspicious e-mails etc. and do not open an email or link if you do not know where it has come from. If you are in doubt then contact the Network Manager by emailing IT Support.

3.4.5 Hardware

- Any damage to hardware or faulty equipment should be reported to the Network Manager immediately
- Students, should, under no circumstances, disconnect any cables from a computer, for example, network, power, mice, keyboards and monitor cables. If for any reason this is required it must only be undertaken by a member of staff
- Network cables should not be removed from wall/floor ports
- No members of Grays Convent High School including staff should disconnect any wireless access points.

4.   Data Protection Act

The school complies with the Data Protection Act 1998 (updated GDPR 2018). The school has a Data Protection Policy. Where students can consent to sharing data, they can also withdraw that consent at any time.

5.   Sanctions

Misuse of Grays Convent High School ICT facilities and the Internet may result in disciplinary action, including verbal and written warnings, withdrawal of access privileges, and in extreme cases, fixed term exclusions or a permanent exclusion. The school also reserves the right to report any illegal activities to the appropriate authorities e.g. the police. Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items that are harmful or banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.   Communication

6.1   Informing Students

Student planners contain a summary of this policy.
Pupils receive lessons (in particular Computing and PSHEC), and assemblies, on e-safety throughout the year in order to increase their awareness of online dangers and to improve their confidence in using the internet safely.

The SENCO and teachers will ensure that the terms of this policy are explained in a clear and helpful way to any pupils with special educational needs who find it difficult to understand.

6.2   Informing Parents/carers

Parents/carers' attention will be drawn to e-safety in the Parent Information Evenings. Advice that accords with acceptable and responsible Internet use, by students at home will be made available to parents. The e-safety policy is available on the school website. Safety issues will be handled sensitively. The school will obtain parental/pupil consent before publication of students' photographs.

6.3 Online Learning Protocol for students

On occasion, some of your teachers might invite you to take part in a "live" lesson using Google Meet. You will need to follow the points below :

-I will remember that all the normal school rules apply when I am learning online. If these rules are not followed, school sanctions will be applied and parent/carers will be informed. You may be removed from the virtual classroom if you do not keep to the rules.

-I will not record or take photos of my classmates or teachers during a video conference lesson/ tutorial. I will only engage in video or audio conversations when my teacher/ tutor invites me to do so.

-I understand that when using applications provided by the school that my use can be monitored and logged and can be made available to my teachers.

-I am aware that when in a live lesson or tutor time that this is an extension of the classroom and I should conduct myself as I would in a classroom.

You must:

· Have your lesson/tutorial in an environment that is quiet, safe and free from distractions but preferably in a common area of your house which is not your bedroom.

· Be on time and mute your microphone when joining.

· Have a neutral (plain) background. Check that there is nothing personal on show behind you for example on your wall.

· Be dressed appropriately for learning as you would be at school (no pyjamas or clothes with inappropriate slogans)

· Remain attentive during sessions without distractions

· Not use the chat function of the platform unless asked to do so by your teacher

· Follow the instructions of your teachers during these live sessions

· Interact patiently and respectfully with your teachers and peers.

· Make sure you end the session as soon as the teacher indicates to do so.

6.4 Review

This policy will be reviewed annually.

Linked policies :
- ICT E-Safety Acceptable use policy for staff
- Remote learning policy
- Data Protection policy
- Behaviour policy
- Safeguarding and child protection policy