Grays Convent

HIGH SCHOOL

ICT E-Safety & Acceptable Use Policy for Staff

This Policy was reviewed and adopted by the Governing Body on 22nd January 2024.

This Policy is 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 staff will benefit from learning and teaching opportunities offered by the school's Internet resources in a safe and effective manner.

WHEN USING GRAYS CONVENT SCHOOL INFORMATION AND COMMUNICATION TECHNOLOGY EQUIPMENT THERE SHOULD BE NO EXPECTATION OF PRIVACY.

Internet use and access is considered a school resource. Access is a privilege, not a right. By accessing the internet using school facilities, staff agree 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 Therefore, if the school policy is not adhered to this privilege will be withdrawn and appropriate sanctions outlined in this policy will be imposed. These statements apply to all staff members.

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

Inappropriate

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

- 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' other than those deemed as having educational value
- Using messenger services 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 (with the exception of the Headteacher to carry out interviews).
- No inappropriate files may be intentionally downloaded. No programs may be introduced, nor installations made without authorisation from the ICT Network Manager
- Downloading and/or distributing music files are not permitted except where it is an integral part of your curriculum 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

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

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

Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted in writing at the Headteacher's discretion.

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 staff 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 the ICT Network Manager or, in their absence, an Assistant / Deputy Headteacher
- Will use the Internet for work related purposes only
- Will not upload, download or otherwise transmit material that is copyrighted
- Will not disclose or publicise personal or confidential information regarding students or other members of staff without seeking approval from their line manager, and appropriate obtain permissions
- Will accept that the school will obtain parental consent before publication of students' photographs. It is the responsibility of staff members to check that permission has been obtained prior to using photos of students in any form of publication
- 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
- Will be aware that all Internet use is logged and access to any inappropriate web sites will be blocked. Grays Convent School does not expect its staff to visit any inappropriate sites. If staff become aware of inappropriate sites that are not picked up by filters and are accessible on the school system, it is their responsibility to inform the Network Manager or, in their absence, the Assistant Headteacher (ICT).
- Must not use the school computer system for personal use e.g. buy and sell items or book holidays. This can lead to security issues.

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 or Google Classroom belongs to the school. Permission to reproduce any other material will be sought and obtained, from the copyright owner through the Headteacher
- The contact details for the school will include only the school's postal address, e-mail address and telephone number. No information about teachers' home addresses or the like will be published
- The publication of students' work will be co-ordinated by a teacher after seeking the approval of their line manager and the appropriate permissions

- Only pictures of pupils at Grays Convent are to be added to the school website with permission of a parent/carer
- Our website contains the CEOP report button and we take part in the Safer Internet Campaign

3.2 E-mail

Grays Convent School encourages staff 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 using Outlook. Staff must not use free e-mail sites such as Yahoo or Hotmail for any school related purpose. 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.

Members of Staff at Grays Convent School

- Will ensure that, in line with Child Protection guidance, any e-mail communication with students or parents/carers will be carried out through school e-mail accounts only
- 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

A member 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.

A member of the school must not say anything in an email that he/she would not be prepared to say in a letter (on the School's headed paper) sent to the same person.

The school email system must 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.

Staff must not give out personal details e.g. address via the e-mail system to pupils or parents.

3.3 Social Networking, Instant Messaging & Chat Rooms

- Staff must not use social networking sites, chat rooms, forums or blogs to post inappropriate or derogatory comments about pupils, parents, other staff members 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 in or out of school may result in disciplinary action
- Staff may use Twitter only to provide information such as revision tips for pupils. It is to be a one way communication taking the form of a message board. Any member planning to set up such a notice

board must seek the Headteacher's consent. No notice board shall be set up until the Headteacher has given consent.

- Staff must not have pupils or parents in their "friend" lists. This is a CEOP requirement
- Staff must not give out information or views that contradict school policies.
- Concerns regarding the online conduct of any member of Grays Convent HIgh School community on social media, should be reported to the DSL (or deputy) and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Staff Personal Use of Social Media :

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities. Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.
- Reputation – All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. This will include (but is not limited to): Setting the privacy levels of their personal sites. Being aware of location sharing services. Opting out of public listings on social networking sites. Logging out of accounts after use. Keeping passwords safe and confidential. Ensuring staff do not represent their personal views as that of the setting. Members of staff are encouraged not to identify themselves as employees of Grays Convent High School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members. All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework. Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites. Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.
- Communicating with students and parents and carers - All members of staff are advised not to communicate with or add as 'friends' any current or past students or their family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the Headteacher. If ongoing contact with students is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools. Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher/line manager. Any communication from students and parents received on personal social media accounts will be reported to the DSL (or deputies).
- For school use all other forms of internet based Instant Messaging are prohibited, for example MSN Messenger, Facebook, AOL IM and Yahoo IM and Skype (with the exception of the Headteacher for interviewing staff and with the exception of Google Classroom)

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 or a memory stick then this will be your responsibility and must not transfer viruses onto the school system. Staff are encouraged to use school email and Google Classroom for file sharing.
- 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
- Official sensitive, confidential data should not be stored on memory sticks or external devices. All staff will have a personal directory. Although under normal circumstances the Network Manager will not access these directories users must be aware that Grays Convent School reserves the right to review what is in these directories for security and legal reasons. Staff are reminded that files or programs that have already been mentioned as forbidden in school should not be brought in from home via a USB memory stick
- MP3, MP4, WMA and other compressed media file formats are not allowed to be stored on Grays Convent School owned ICT resources, unless they are required for educational purposes
- Staff must make regular backups of all their school work held on laptops or non school computers. This must be secure and password protected.

3.4.2 Usernames, Passwords and Security

- You will be issued a username and password for email, Google Classroom and the school network. This is to be kept secure and changed regularly.
- 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 School
- If you suspect other persons have your password then please inform the ICT Network Manager
- 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
- To comply with the Data Protection Act, if you are temporarily leaving your workstation or laptop unattended for any length of time you must either lock the workstation or laptop to ensure it is password protected or log off
- Use of another person's individual 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 legal action. Student data help on laptops must be encrypted

3.4.3 Unauthorised Software

- No unauthorised software is to be loaded. If you are unsure as to what is deemed to be unauthorised, then please contact the Network Manager
- If you require anything in addition to what is 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.
- Staff must not switch off or change the settings of the virus shield on their school laptop for any reason
- Staff must update anti virus and malware software installed by the school on their laptops regularly.
- Ransomware - A Ransomware attack is when someone hacks into the computer system and stops it from functioning and/or steals data from it and demands money in order for access to be re-gained. It is usually started when someone clicks on a link which causes the computer to crash and then spreads across the whole system. Computers are then out of action for weeks and may even need to be replaced. Please make sure you know what to do should this happen and **report it immediately** to The Headteacher (PJ), Assistant Headteacher (POH) and IT Support as emergency action would be needed.
- In the event of this happening the procedure to follow would be :
- **Turn off the computer at the wall and report it to ITSupport and POH or PJ immediately. The quicker ITSupport know about it, the easier it is to resolve. The longer the attack lasts the more likely it is that it will spread across the whole system and that data will be lost and we will not be able to regain access.**

- Please be extra vigilant and as always only click links and download from known sources. If something doesn't look right, don't trust it. If you are working from home, please make sure that your anti-virus software is up to date. If you receive an unusual looking email, don’t open it. Please delete it from your inbox and then delete it again from your bin.

3.4.5 Hardware

- Staff who disconnect any cable from a computer, for example, network, power, mice, keyboards and monitor cables should ensure that the equipment is returned to its original state after use
- Any damage or faults must be reported to Network Manager immediately
- Network cables should not be removed from wall/floor ports
- Staff must not disconnect computers set up for whiteboard use and replace them with their own laptops
- No members of staff should disconnect any wireless access points.

4. Data Protection Act

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

5. Sanctions

Misuse of Grays Convent School ICT facilities and the Internet may result in disciplinary action, including verbal and written warnings, withdrawal of access privileges, and in extreme cases, suspension from duty. Any serious misuse is gross misconduct and may result in dismissal. The school also reserves the right to report any illegal activities to the appropriate authorities.
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. Two members of staff should be present for such a search including a Head of Year or member of SLT.

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 Staff

All staff will be provided with access to a copy of the School's Acceptable Use Policy. Teachers are aware that Internet traffic can be monitored and traced to an individual user. Staff will be consulted about the development or the school's Acceptable Use Policy and instructions on safe and responsible Internet use.

6.2 Remote learning

All staff need to encourage students to follow the online learning protocol and consider how if affects them when they teach remotely.

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.

Glossary

Proxy	Students may use a proxy site to gain access to websites that are forbidden in school as the proxy server will act as an intermediary. Proxy servers can also be used to anonymize e-mails or by hackers to 'eavesdrop' on information being sent over the Internet.
ISP	Internet Service Provider
Skype	An Internet telephony service
AOL IM	America Online's instant messaging service (similar to MSN Messenger)
MP3 & MP4	Compressed audio files
WMA	Windows Media Audio file
Zip files	A compressed file

CEOP	The Police organisation - Child Exploitation and On-line Protection
Twitter	An online social networking and micro blogging service that enables its users to send and read text-based messages of up to 140 characters, known as "tweets".

6.3 Review

This policy will be reviewed annually by the Assistant Headteacher.

Linked policies :

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