Dominican College

E-safety Policy

Updated: September 2022

Review: Bi-annually(*by E-safety Coordinator*)

Contents

CONTENTS **2**

1. RATIONALE **3**

2. AIM & OBJECTIVES **3**

3. ROLES & RESPONSIBILITIES **3**

MAIN E-SAFETY ROLES & RESPONSIBILITIES AT DOMINICAN COLLEGE 4

4. POLICY STATEMENTS **5**

A. EDUCATION – PUPILS 5

B. EDUCATION – PARENTS / GUARDIANS 5

C. EDUCATION – THE WIDER COMMUNITY 5

D. EDUCATION & TRAINING – STAFF / VOLUNTEERS 6

E. TRAINING – GOVERNORS 6

F. TECHNICAL – INFRASTRUCTURE / EQUIPMENT, FILTERING AND MONITORING 6

(i) General: Infrastructural & Equipment *6*

(ii) Filtering *7*

G. ACCEPTABLE USE OF THE INTERNET 7

(i) Use of the Internet *7*

(ii) Access to the Internet *8*

(iii) Use of email *8*

H. BRING YOUR OWN DEVICE (BYOD) 9

I. USE OF DIGITAL AND VIDEO IMAGES 9

J. DATA PROTECTION 9

(i) Overview *9*

(ii) Password Security *10*

(iii) Electronic Storage Devices *10*

K. MOBILE/PORTABLE TECHNOLOGY 10

L. COMMUNICATIONS 11

M. SOCIAL MEDIA / NETWORKING 12

(i) Staff (including governors): Protecting Professional Identity *12*

(ii) Pupils: Child Protection *13*

N. UNSUITABLE / INAPPROPRIATE ACTIVITIES 13

O. RESPONDING TO INCIDENTS OF MISUSE 13

(i) Illegal Incidents *13*

(ii) Other Incidents *14*

P. SCHOOL ACTIONS & SANCTIONS 14

5. OTHER RELEVANT POLICIES **14**

6. APPENDICES **15**

RECORD OF REVIEWING DEVICES / INTERNET SITES (RESPONDING TO INCIDENTS OF MISUSE) **15**

TEMPLATE REPORTING LOG **16**

DOMINICAN COLLEGE'S STANCE ON SOME OF THE MAIN FORMS OF COMMUNICATION **17**

UNSUITABLE / INAPPROPRIATE ACTIVITIES **18**

POTENTIAL SCHOOL ACTIONS AND SANCTIONS ASSOCAITED WITH E-SAFETY INCIDENTS **19**

REFERENCES **21**

1. Rationale

This policy applies to all members of the *School*[1] (including staff, pupils, volunteers, parents / guardians, visitors, community users[2]) who have access to and are users of school Information Communication and Technology (ICT) systems, both in and out of the School. ICT includes a wide range of resources such as web-based and mobile learning. The table below, while not exhaustive, lists some of the core technologies that young people are currently using both inside and outside of the classroom.

Websites	**Music Downloading**	**Gaming**
Email and Instant Messaging	**Blogs**	**Podcasting & Video Broadcasting**
Chat Rooms and Social Networking such as Facebook and Twitter	**Mobile/Smart phones with text, video and/ or web functionality**	**Other mobile devices (such as iPads, Kindle, etc.) with web functionality**

We recognise and value the increasingly wide opportunities that ICT provides to our staff and pupils. Whilst it is our aim that all members of our school community avail as fully as possible of this technology we also appreciate the need for safeguards to be in place. Young people have many opportunities to benefit from what are becoming very sophisticated hand-held devices outside school.

The Principal and staff have a duty of care to the pupils at Dominican College and as such will impose (if necessary) disciplinary penalties for inappropriate online / technologically-based behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place inside or outside of the school.

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

Please note that school policies rarely act in isolation of each other. Good practice necessitates robust policies which are intertwined with one another to ensure maximum benefits and protections are afforded to all stakeholders. Section 4 lists other policies that operate alongside this policy.

2. AIM & Objectives

Our aim is to highlight the responsibility of everyone in Dominican College to consider e-safety and to mitigate risk through reasonable planning and actions. **ALL key stakeholders will be expected to abide by the E-safety Policy (see website for E-safety Policy).** E-safety covers not only internet technologies but also electronic communications via mobile devices[3], games consoles and wireless technology.

E-Safety in the school context:

- is concerned with safeguarding young people in the digital world;
- emphasises learning to understand and use (new) technologies in a positive way;
- focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school;
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.
- both this policy and associate Acceptable Use Policies are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, iPads, webcams, digital video equipment, etc.); and technologies owned by pupils and staff, brought onto school premises (e.g. mobile phones, etc.).

3. Roles & Responsibilities

See the next page for an overview of the main e-safety roles and responsibilities at Dominican College.

---

[1] *From this point on the 'School' may be used to mean Dominican College.*

[2] *May be referred to on occasion as 'stakeholders'.*

[3] For School use '*mobile devices*' refers to tablets or laptops NOT mobile phones.

Main E-safety Roles & Responsibilities at Dominican College

Board Of Governors (BOG)

- Approve & review the effectiveness of the E-safety Policy
- Appoint an e-safety Governor, who will regularly meet with the ESC and CPO.
- They will also review the e-safety incident logs, review filtering, report to the whole BOG and attend relevant meetings/training

Principal & SLT

- Select and meet regularly with the ESC
- Be aware of the e-safety procedures to be followed, if an incident is reported (see sub-section 'O')
- Promote and secure training for relevant staff
- Ensure monitoring and support is available for staff with an e-safety role

E-safety Coordinator (ESC)

- Lead person with day-today responsibility for e-safety who liaises regularly with all key stakeholders, especially the CPO
- Ensures documents are up-to-date along with promoting e-safety awareness, advice & training
- Creates & monitors the e-safety log
- Attend relevant meetings/training and report regularly to the SLT and e-safety governor

Network Manager/ICT Coordinator

- Will ensure the school's technical infrastructure (in partnership with C2k) is monitored and security meets local authority and ESP requirements
- Ensures users may only access school resources through password secure systems and appropriate filtering is always in place
- Assists with the e-safety log and attends relevant meetings/training

E-safety Committee (Meet 1-2 times per year)

- Will review and recommend ESP changes; which will take into account local, national and global trends and demands
- School e-safety resources, literature, training, links with third-parties will be reviewed and updated where necessary
- Review e-safety log and respond to any critical issues

Child Protection Officer (CPO)

- Should be trained in e-safety issues and be aware of and monitor the following issues – sharing of personal data, access to illegal/inappropriate materials, inappropriate online contact with adults/strangers, potential or actual incidents of grooming, sexting or cyber-bullying.

Parents

- Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way
- Parents/Guardians are encouraged to support the school in promoting good e-safety practice and to help ensure their child follows guidelines on the appropriate use of digital images/video, internet use and technology including mobile devices
- Can obtain e-safety information from the School website or by contacting the ESC

Pupils

- Must use digital technology in accordance with the school's AUPs. The school's ESP also covers pupils' actions out of school, if directly related to their membership of the school
- Take responsibility for developing research skills and the need to avoid plagiarism and uphold copyright laws
- Needs to understand the importance of reporting abuse, misuse or inappropriate materials

Teaching & Support Staff

- Should have an up-to-date awareness of e-safety and of the current school E-safety policy and other relevant AUPs. Staff should also help ensure pupils follow and understand the AUPs
- Monitor and report any suspected or actual misuse of technology or the internet to the ESC or a Senior Teacher
- All digital communication associated with school should be carried out using official school systems and emails. The transferring of data must only be done using encrypted devices
- In lessons where internet use is pre-planned pupils should be guided to suitable pre-checked sites

NB: ***All stakeholders have a duty of care and must ensure that personal and sensitive data is protected at all times in keeping with the School's Data Protection Policy.***

4. Policy Statements

a. Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in ALL areas of the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and may be provided in the following ways:

- A planned e-safety curriculum should be provided as part of every lesson where technology and online activity takes place. Lesson plans should be regularly revisited, and where appropriate pupils taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreements and encouraged to adopt safe and responsible use both within and outside school;
- Staff should act as good role models in their use of digital technologies the internet and mobile devices;
- In lessons where internet use is pre-planned, it is best practice that pupils should be 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;
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit;
- It is accepted that from time-to-time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

b. Education – Parents / Guardians

Many parents and guardians have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Where appropriate the School will therefore seek to provide information and awareness to parents and guardians through:

- Curriculum activities;
- Letters, newsletters, website (http://www.dominicancollege.org.uk/), VLEs;
- Parents / Guardians evenings / sessions;
- High profile events / campaigns e.g. Safer Internet Day (7th February 2017);
- Reference to the relevant web sites / publications are regularly updated on our website - http://www.dominicancollege.org.uk/

c. Education – The Wider Community

If appropriate the School will provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives as well as parents;
- The School website may provide e-safety information for the wider community;
- Supporting community groups e.g. Early Years Settings, Child-minders, youth / sports / voluntary groups to enhance their e-safety provision.

d. Education & Training – Staff / Volunteers

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:

- Where suitable and appropriate a planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced;
- All new staff should 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 (or other nominated person) will receive regular updates through attendance at external training events;
- Where appropriate this E-safety policy and its updates will be presented to and discussed by staff during INSET days;
- The E-safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

e. Training – 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 / Governors Associations / or other relevant organisations;
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / school events).

f. Technical – infrastructure / equipment, filtering and monitoring

(i) General: Infrastructural & Equipment

The school has a responsibility to ensure that the managed service provider (C2K) carries out all appropriate e-safety measures.

The School is 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 need to ensure that the following e-safety responsibilities are carried out:

- School systems will be managed in ways that ensure that the school meets recommended technical requirements (these will be in line with the School's Personal Data Handling Policy – available on request);
- There will be regular reviews and audits of the safety and security of school technical systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data;
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (i.e. ICT Technician);
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed regularly, by the E-Safety Committee (or other group);
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (see Password Security section);
- ICT technician and Network Manager are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations;
- Mobile device security and management procedures are in place (where mobile devices are allowed access to school systems);
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement;
- Remote management tools may be used by staff to control workstations and view users activity;

- An appropriate system is in place where users can report any actual / potential technical incident to the E-Safety Coordinator / Network Manager / Technician (see Appendices A & B for responding to incidents of misuse and keeping a Reporting Log);
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system – this is managed by the ICT technician and Network Manager.

(ii) Filtering

- C2K in conjunction with the School provide a filtering service for all Internet and email. However, any filtering service, no matter how thorough, can never be comprehensive, and it is essential that all stakeholders (especially pupils) clearly understand the School's Acceptable Use of the Internet;
- The responsibility for the management of the school's filtering policy will be held by the ICT technician in conjunction with C2K. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems;
- Changes to the School's filtering service must
    - be logged in change control logs
    - be reported to a second responsible person (e.g. Network Manager or E-safety Coordinator) ;
- All users have a responsibility to report immediately to (the ICT technician or Network Manager) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered;
- Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials;
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems;
- The school (ICT technician) / filtering partners will provide where appropriate enhanced / differentiated user-level filtering;
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal (or other nominated senior leader);
- Requests from staff for sites to be removed from the filtered list will be considered initially by the ICT technician and then by the Network Manager or E-safety Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety coordinator;
- Where appropriate staff, pupils, governors and visitors will be given relevant training or information regarding filtering;
- Monitoring of the filtering system will be regularly reviewed by the ICT technician / Network Manager / E-safety Coordinator / nominated Senior Teacher.

g. Acceptable Use of the Internet

(i) Use of the Internet

- When using the Internet, all staff, governors, pupils, and visitors must comply with all copyright, libel, fraud, discrimination and obscenity laws, and are expected to communicate in a manner consistent with the aims and the ethos of Dominican College.
- While the use of information and communication technologies is a required aspect of the Northern Ireland Curriculum, access to the Internet and My School remains a privilege not a right. It is given to those who act in a considerate and responsible manner, and will be withdrawn if they fail to maintain acceptable standards of use.
- No Internet user is permitted to:
    (a) Retrieve, send, copy or display offensive messages or pictures;
    (b) Use obscene or racist language;
    (c) Harass, insult or attack others;
    (d) Damage computers, computer systems or computer networks;
    (e) Violate copyright laws;
    (f) Use another user's password;
    (g) Trespass in another user's folder, work or files;
    (h) Intentionally waste resources (such as on-line time and consumables);
    (i) Use the school network for unapproved commercial purposes.
    (j) Use the school network for private or personal purposes.
- Use of online resources by pupils of Dominican College must be in support of the aims and objectives of the Northern Ireland Curriculum.
- Electronic information handling skills are now fundamental to the preparation of citizens and future employees in the information age. Staff are encouraged to investigate the possibilities provided by access to this electronic

information and communication resources, and blend its use, as appropriate, within the curriculum. They will, wherever possible, model appropriate and effective use, and provide guidance and instruction to pupils in the acceptable use of the Internet.

(ii) Access to the Internet

- Staff:
  - Staff will be given access to the internet primarily for teaching and learning. However; care must be taken when using the internet and showing websites to pupils as staff have less restrictive filtering.
  - Good practice dictates that websites/online content should be viewed and vetted in advance of showing to pupils and in the unlikely event of inappropriate content being viewed the internet should be closed and the issue reported immediately to the ICT technician and/or a senior teacher.
  - A log should be kept of any incidents and the action taken. This needs to be made available to the E-safety Coordinator.
  - During non-contact time staff may use the internet for non-school related tasks (e.g. shopping, holidays, news, etc.) however, their use and the appropriateness of the web content must still comply with this policy.
- Pupils:
  - Pupils will only be given access to the internet on receipt of a signed pro-forma acknowledging that they have read and understand the school's Acceptable Use of the Internet. Parents /Guardians will also be asked to countersign this statement.
  - All internet activity should be appropriate to each pupil's education.
  - Personal User ID's and passwords for use on the computer networks MUST be kept secret.
  - Access should only be made via the authorised account and password, which should not be made available to any other person: the authorised user will be held responsible for all activities in that account.
  - Activity that threatens the integrity of the School's ICT systems, or activity that attacks or corrupts other systems, is forbidden.
  - Users are responsible for all email sent and for contacts made that may result in email being received.
  - Use for personal financial gain, gambling, political purposes or advertising is forbidden.
  - Copyright of materials must be respected.
  - Posting anonymous messages and forwarding chain letters in forbidden.
  - As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters and other media.
  - All emails sent and received are filtered for content. Emails which are filtered and blocked are stored and are available for viewing by the Principal. All users should be aware that emails sent or received can be accessed and viewed where it is felt necessary. Blocked emails can be 'released' by filling in a proforma available in the Office – all other blocked emails will be automatically deleted four weeks after being blocked.
  - Use of the network to access inappropriate materials such as pornographic, racist or other offensive material is forbidden.
  - Violations of the above rules will be regarded as a major breach of school discipline and will result in a temporary or permanent ban on internet use.
  - Additional disciplinary action may be added in line with existing practice.

(iii) Use of email

All emails sent and received are filtered for content. Emails which are filtered and blocked are stored and are available for viewing by the Principal. All users should be aware that emails sent or received can be accessed and viewed where it is felt necessary. Blocked emails can be 'released' by filling in a proforma available in the Office – all other blocked emails will be automatically deleted four weeks after being blocked.

- Staff:
  - Email is of great value; however the School expects staff to maintain a strict demarcation between their private/personal email and their professional/work email.
  - Work email should be the ONLY email used in connection with work (e.g. communicating with staff, pupils, examination boards, etc.).
  - As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters and other media.
  - There is an expectation that staff will regularly use and check their email (e.g. daily during the academic year) and respond in a timely fashion is it is appropriate to do so.
  - If necessary the Principal (or a Senior Teacher named by the Principal) may monitor or access school email accounts.
- Pupils:
  - Pupils are only permitted to use the email service provided by C2K on the school network.

- Use, by pupils, of other web based email providers such as Hotmail is strictly prohibited.
- Posting anonymous messages and forwarding chain letters in forbidden.

h. Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. Where appropriate the School may allow pupils to bring their own mobile device (mobile phones are NOT permitted) into school for use school only. All pupils will be automatically enrolled in the BYOD scheme, unless they opt-out in writing and countersigned by a parent/guardian. The BYOD policy is available on the School's website.

i. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / guardian and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. Digital images may remain available on the internet indefinitely and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes;
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- Pupils must not take, use, share, publish or distribute images of others without their permission and the permission of a teacher;
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- Written permission from parents or guardians will be obtained before photographs of pupils are taken;
- Pupil's work can only be published with the permission of the pupil and parents or guardians.
- Any pupil who has opted out of having their photograph taken for school use has responsibility to identify themselves to a member of staff either before or at the time the image/video is being taken.

j. Data Protection

(i) Overview

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
- Every effort will be made to ensure that data held is accurate, up-to-date and that inaccuracies are corrected without unnecessary delay.
- It has a Data Protection Policy;
- Risk assessments are carried out where appropriate;
- It has clear and understood arrangements for the security, storage and transfer of personal data;
- Data subjects have rights of access and there are clear procedures for this to be obtained;
- There are clear and understood policies and routines for the deletion and disposal of data;
- There is a policy for reporting, logging, managing and recovering from information risk incidents;
- Where cloud storage is used the school, in conjunction with C2K, will regularly check and maintain data security.

(ii) Password Security

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the ICT technician and/or Network Manager and will be reviewed regularly by the E-Safety Committee.
- Passwords for new users, and replacement passwords for existing users will be allocated by the ICT technician.
- All users (adults and young people) will
- Staff passwords:
    - all staff users will be provided with a username and password by the ICT Technician who will keep an up-to-date record of users and their usernames.
    - the password should be in line this current C2K guidance for setting new password (available from the ICT technician).
    - the account will be "locked out" following a number of successive incorrect log-on attempts
    - temporary passwords – should be changed as soon as possible.
    - passwords shall not be displayed on screen, and shall be securely hidden.
    - passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
    - staff have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
    - should be changed when prompted by C2K.
- Pupil passwords:
    - all users will be provided with a username and password by the ICT technician who will keep an up-to-date record of users and their usernames.
    - users will be required to change their password when prompted by C2K.
    - pupils will be taught the importance of password security
    - The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.
    - pupils have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

(iii) Electronic Storage Devices

- When personal data is stored on any portable computer system, memory stick or any other removable media, staff must ensure:
    - the device must be password protected;
    - the device must offer approved virus and malware checking software;
    - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

k. Mobile/Portable Technology

- Mobile Phones are Not to be used by pupils at any stage during the school day.
- Mobile devices are not allowed to be used in school unless they are part of a school initiative and pupils have been authorised to use the device by a member of staff (if this is the case then pupils are bound by the BYOD Policy – available on the School's website). In the event of a pupil caught using a mobile device without permission he/she will be asked to hand it to a member of staff; the device will then be left at reception and to be collected by a parent / guardian. Severe breaches will be referred immediately to a Head of Year or Senior Teacher.
- Heads of Year and Senior Teachers are authorised to carry out searches for mobile devices where they reasonably suspect that the data or file (e.g. audio-visual or text) on the device in question has, or could be, used to cause harm, to disrupt teaching or break school rules.
    - Searching with consent - Authorised staff may search with the pupil's consent for any item – it is good practice to have a second member of staff present.
    - Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' or appears in the school rules as an item which is banned and may be searched for. In carrying out the search:

- The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.
- The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.
- The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the pupil being searched.
- The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member).
  - There is a limited exception to this rule: Authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.
- The person conducting the search may not require the pupil to remove any clothing other than outer clothing. Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
- A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

NB1: The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

NB2: Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

- An authorised member of staff finding a mobile device may access and examine any data or files on the device if they think there is a good reason to do so. The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident.
- If inappropriate material is found on the device it should be given to the E-safety Coordinator (or a Senior Teacher) who will investigate further in accordance with this policy.
- Following an examination of an electronic device, if the E-Safety Coordinator (or Senior Teacher) has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules). A record should be kept of the reasons for the deletion of data / files. If the inappropriate material is potential criminal in nature then it should not be deleted and instead be referred to the relevant authorities (e.g. the police).
- School staff should ensure that surrendered devices are kept safe, to avoid the risk of compensation claims for damage / loss of such devices.
- The responsible person confiscating the device or deleting material will keep a record of their actions and give a copy to the E-safety Coordinator.

l. Communications

(i) There is currently a wide range of rapidly developing communications technologies which have the potential to enhance learning. The school will review the suitability and appropriateness of each on a case-by-case basis. Appendix C shows how the school currently views some of the main developing technologies:

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

- The official school email service and Microsoft Teams may be regarded as safe and secure and is monitored. Users should be aware that email communications and Microsoft Teams are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access);
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, 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 /guardians (email, chat, VLEs, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications;

- Pupils will be provided with individual school email addresses for educational use;
- 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.

m. Social Media / Networking

Social networking is growing in popularity, and is used by many to keep in touch with family, friends and colleagues on a social basis. While in the vast majority of cases, the use of such sites is trouble free, guidance to staff, governors and volunteers of Dominican College is required. This policy provides guidance to staff and pupils on their personal responsibility as an employee or pupil of Dominican College when using any social networking site.

Social networking activities conducted on-line outside working hours such as blogging (writing personal journals to internet pages which are publicly accessible), involvement in social networking sites such as TikTok, Facebook, Myspace, Instagram, Snapchat, BeReal, Messenger, Twitter or Bebo and posting material, images or comments on sites such as YouTube, Tumblr and Flickr can have a negative effect on the reputation or image of the school. In addition Dominican College has a firm commitment to safeguarding pupils and staff in all aspects of its work.

(i) Staff (including governors): Protecting Professional Identity

- Key Principles:
  - Every member of staff, governor, or volunteer has a responsibility to ensure that they protect the reputation of the school and to treat colleagues and members of the school with professionalism and respect.
  - It is important to protect every member of staff, governor or volunteer at the School from allegations and misinterpretations which can arise from the use of social networking sites.
  - Safeguarding pupils is a key responsibility for all members of staff, governors and volunteers and it is essential that everyone considers this and acts responsibly if they are using social networking sites out of school. No-one who works in the school either as a paid employee or volunteer must communicate with pupils via social networking.
  - This policy relates to social networking outside work; blogging and accessing social networking sites at work using school equipment is NOT permitted.
  - No communications relating to any specific event, protocol, pupil or person at the School should be shared, irrespective of their anonymity.
- Code of Conduct:
  - The following are not considered acceptable:
    - Use of the school's name, logo, or any other published material without prior written permission from the Principal. This applies to any published material including the internet or written documentation.
    - The posting of any communication or images which link the school to any form of illegal conduct or which may damage the reputation of the School. This includes defamatory comments.
    - The disclosure of confidential or business-sensitive information or the disclosure of information or images which could compromise the security of the school.
    - The posting of any images of employees, pupils, governors or other persons directly connected with the school while engaged in school activities.
  - In additional all members of staff, governors and volunteers must ensure that they:
    - Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school or anyone connected with the School.
    - Use social networking sites responsibly and ensure that their personal or professional reputation, or the school's reputation, is not compromised by inappropriate postings.
    - Are aware of the potential of on-line identity fraud and are cautious when giving personal information about themselves which may compromise their personal safety and security.
    - Do not communicate with any pupil studying at the School through a social networking site.
    - Do not use social media in any way which is unlawful.

NB 1: The above statements refer to the posting of ALL types of content on social media sites including (but not exclusively) text, photographs and video.

NB 2: With the exception of immediate family members it is recommended that staff, governors and volunteers should not communicate with any child (under 18 years old) via a social network site. Where family members under 18 are accessible through social networking site, staff governors and volunteers should ensure their privacy settings are routinely checked to prevent third party access.

(ii) Pupils: Child Protection

For the purpose of Child Protection/ Safe Guarding:

- Pupils are not permitted to engage with or access any social networking site while on school premises. This applies to all school-based facilities and personal technologies.
- Pupils should not make any derogatory, defamatory, rude, threatening or inappropriate postings about the school, or anyone (e.g. other pupils, staff governors, volunteers, visitors etc.) connected to the school. Note that 'postings' refer to ALL types of content on social media sites including (but not exclusively) text, photographs and video.
- In the event that a pupil breaks the above regulations parents/guardians will be contacted and the pupil may be subject to sanctions.

n. Unsuitable / Inappropriate activities

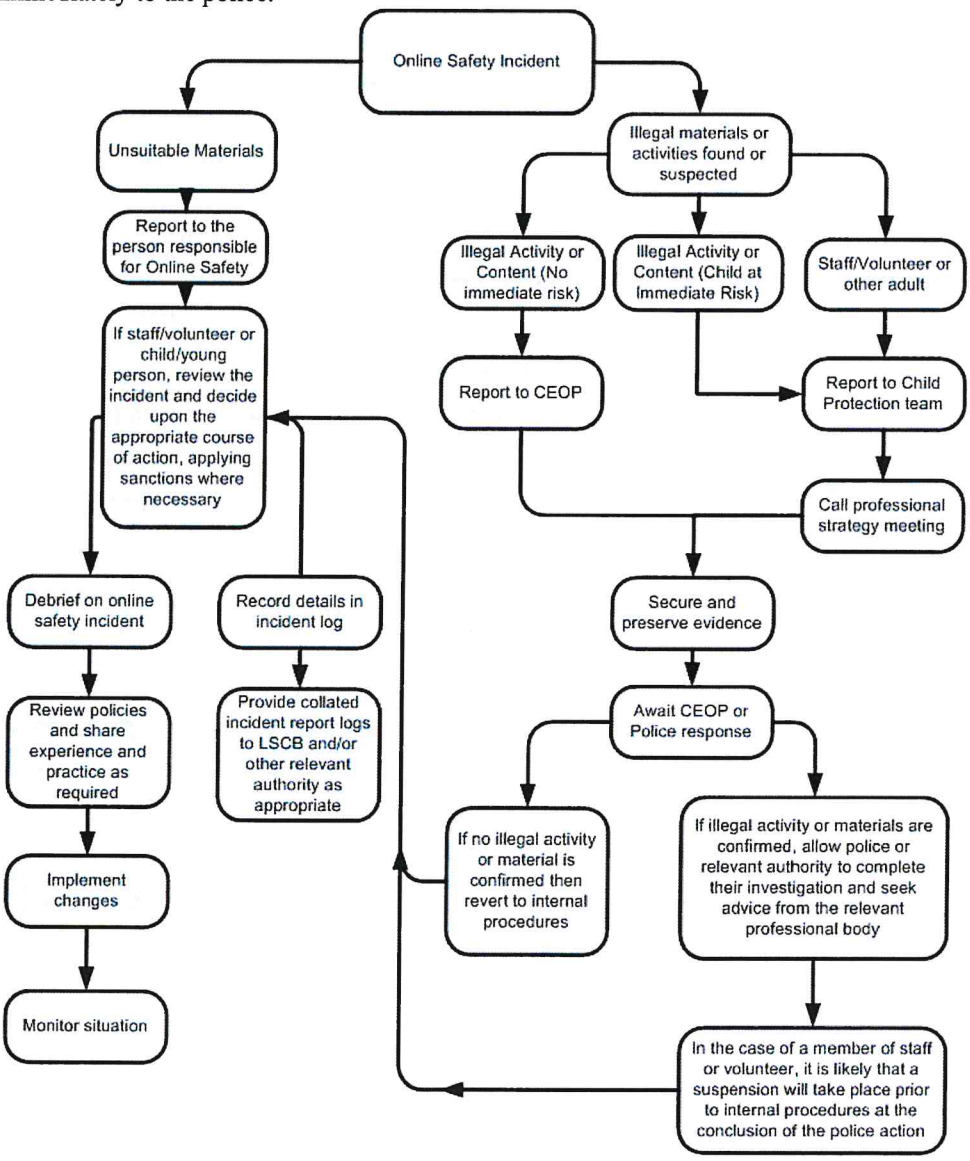
The school believes that the activities referred to in Appendix D would be inappropriate in a school context and that users, should not engage in these activities in school or outside school when using school equipment or systems.

o. Responding to incidents of misuse

See Appendices A & B for responding to incidents of misuse and keeping a Reporting Log

(i) Illegal Incidents

- If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



(ii) Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported;
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure;
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection);
- Record the ***url*** of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below);
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures;
    - Involvement by Local Authority or national / local organisation (as relevant);
    - Police involvement and/or action.
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour;
    - the sending of obscene materials to a child;
    - adult material which potentially breaches the Obscene Publications Act;
    - criminally racist material;
    - other criminal conduct, activity or materials;
    - Isolate the computer in question as best you can. Any change to its state may hinder a later police; investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

p. School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. Appendix E provides, by way of example, an overview of how some incidents may be dealt with.

5. Other Relevant Policies

The following policies are interrelated with the E-safety Policy; as such they should be viewed in conjunction with the E-safety policy:-

- Code of Conduct – Staff & Pupils
- Positive Behaviour Policy
- Acceptable use of the Internet
- Anti-bullying Policy (incorporates cyber-bullying)
- Data Protection Policy
- Policy on the Acceptable Use of Computers, Mobile Technology & the Internet
- BYOD Policy

Other relevant information includes:-
- The School Website (http://www.dominicancollege.org.uk/)

6. Appendices

Appendix A

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

Appendix B

Template Reporting Log

Reporting Log
Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Appendix C

Dominican College's stance on some of the main forms of Communication

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	●				●			
Use of mobile phones in lessons				●				●
Use of mobile phones in social time	●							●
Taking photos on mobile phones / cameras				●				●
Use of other mobile devices e.g. tablets		●					●	
Use of personal email addresses in school, or on school network		●						●
Use of school email for personal emails				●				●
Use of messaging apps		●					●	
Use of social media (for personal use)		●						●
Use of Microsoft Teams	●				●			
Use of social media (for school use – e.g. Twitter)		●					●	
Use of blogs		●					●	

NB: This list is not exclusive or exhaustive. All new forms of communication will be reviewed on a case-by-case basis.

Appendix D

Unsuitable / Inappropriate Activities

The school's E-safety policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		
File sharing				X		
Use of social media					X	
Use of messaging apps				X		
Use of video broadcasting e.g. Youtube				X		

NB: This list is not exclusive or exhaustive. When an incident of unsuitable or inappropriate misuse of technology is reported or identified an investigation will be carried out in a case-by-case basis.

Appendix E

Potential School Actions and Sanctions assocaited with E-safety Incidents

Pupils	**Possible Actions / Sanctions**								
Incidents:	Refer to class tutor	Refer to Head of Department / Head of Year / Senior Teacher	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / guardians	Removal of network / internet access rights	Warning	Further sanction e.g detention / exclusion.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X			X			X	
Unauthorised use of mobile phone / digital camera / other mobile device		X				X			X
Unauthorised use of social media / messaging apps / personal email		X			X	X			
Unauthorised downloading or uploading of files		X			X	X		X	
Allowing others to access school network by sharing username and passwords		X			X	X	X	X	
Attempting to access or accessing the school network, using another pupil's account		X	X		X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff		X	X		X	X	X	X	X
Corrupting or destroying the data of other users		X	X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X		X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X		X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system		X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

NB: This list is not exclusive or exhaustive. When an incident of unsuitable or inappropriate misuse of technology is reported or identified an investigation will be carried out in a case-by-case basis.

Staff **Possible Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Principal	Refer to SLT	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X		X		X	X		
Unauthorised downloading or uploading of files	X		X		X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X		X	X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X	X		X	X		X
Deliberate actions to breach data protection or network security rules	X	X	X		X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X	X		X	X		X
Actions which could compromise the staff member's professional standing	X	X	X		X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X		X
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X	X

NB: This list is not exclusive or exhaustive. When an incident of unsuitable or inappropriate misuse of technology is reported or identified an investigation will be carried out in a case-by-case basis.

REFERENCES

Below are a list of websites, which provided useful information and resources, vital to the creation of our E-safety Policy.

https://saferinternet.org.uk/
https://swgfl.org.uk/online-safety/
https://360safe.org.uk/
https://www.safeguardingni.org/
https://www.ceop.police.uk/Safety-Centre/
https://www.thinkuknow.co.uk/
https://www.childnet.com/
https://www.internetmatters.org/resources/esafety-leaflets-resources/
https://www.education-ni.gov.uk/publications/e-safety-guidance
https://www.getsafeonline.org/