DUNCLUG COLLEGE

AD VITAM PARAMUS

Online Safety Policy

"The welfare of our children is paramount"

Contents

1.0 Developing and Monitoring this Policy
2.0 Roles and Responsibilities
3.0 Policy Statements
    3.1 Online Safety
    3.2 Technical
    3.3 Bring Your Own Device (BYOD)
    3.4 Use of Images and Video
    3.5 Data Protection
4.0 Communications
5.0 Appendices

1.0 Development & Monitoring of this Policy

This online safety policy has been developed by a the **E-Learning Group**
Consultation with the whole school has taken place.

Schedule for Development/Monitoring/Review

Approved by the Board of Governors:	*June 2021*
The implementation of this online safety policy will be monitored by the:	*School Development Group*
Monitoring will take place at regular intervals:	*Annually - in June*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.	*Annually - in June of each academic year*

The school will monitor the impact of the policy using a combination of:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of pupils, parents/carers and staff

Related School Policies

Data Protection Policy | Safeguarding Policy | Blended Learning Policy

2.0 Roles and Responsibilities

Board of Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

Principal & SLT

- The Principal has a duty of care for ensuring the safety (including online) of members of the school community.
- The Principal and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles.
- The Strategic Leadership Team will receive regular monitoring reports from the Online Safety Lead.
- The member of SLT with responsibility for e-learning, the Director of Evaluation and Development, leads the E-Learning Group, takes responsibility for online safety responsibilities, takes a lead in reviewing policy, liaises with Head of ICT and technical support staff, receives reports of online safety incidents, maintains a log and reports regularly to the SLT.

C2K Managers & School Technicians

Those with technical responsibilities are responsible for ensuring:

- that the technical infrastructure is secure and is not open to misuse or malicious attack and meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal and Senior Leaders
- that monitoring systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have read, understood and signed the staff acceptable use policy (AUP)
- they report any suspected misuse or problem to SLT for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level
- online safety issues are embedded the curriculum and other activities where appropriate
- pupils follow the Online Safety Policy and acceptable use policies
- instructing pupils regarding research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities

Designated Child Protection Officer

Should be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

E-Learning Group

Members take the lead with regards to:

- the production/review/monitoring of the school online safety policy
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision

Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials
- will be expected to know policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying
- should understand the importance of adopting good online safety practice and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Dunclug College will take every opportunity to help parents understand these issues. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in the school

3.0 Policy Statements

3.1 Dunclug College Online Safety curriculum

The education of pupils in online safety & digital literacy is an essential part of the Dunclug College's online safety provision. Pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in many areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PSE/other schemes of work
- Online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the validity of content they access on-line
- Pupils should be taught to acknowledge the source of information used and to respect copyright
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- Where pupils are allowed to search the internet, staff should be vigilant in monitoring
- It is accepted that from time to time, for good educational reasons, students 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 technicians can temporarily remove those sites from the filtered list for the period of study.
- Inform parents about online safety through curriculum activities, social media, meetings and Safer Internet Day.

3.2 Filtering and monitoring through the managed C2K network

Dunclug College will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- 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
- All users will have clearly defined access rights to college technical systems and devices
- All users will be provided with a username and secure password. Users are responsible for the security of these.
- C2k Manager and Staff passwords will be kept securely and not "shared".
- Internet access is filtered for all users. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Dunclug College has provided enhanced/differentiated user-level filtering.
- Technical staff regularly monitor and record the activity of users on the school systems.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off site unless safely encrypted or otherwise secured.

3.3 Mobile Technologies (including BYOD)

- All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational.
- The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies.

- The BYOD Acceptable Use Policy should be signed by all pupils before access is given to the school wifi network.
- BYOD can be a great support within school for learners but pupils must be aware that they cannot bring inappropriate electronic data into school on their own device.
- Any device being brought into school is the responsibility of the pupil bringing it in.. The school is not liable for loss, damage or theft of said device.

See the AUA for full details.

3.4 Use of Digital and Video Images

The school will inform and educate users about the risks involved with digital media and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, social media and or local press.
- Parents/Carers are welcome to take videos and digital images of their own children at college events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Dunclug College equipment; the personal equipment of staff should only be used if permission has been granted by SLT.
- Care should be taken that pupils are appropriately dressed and are not participating in activities that might bring the individuals or Dunclug College into disrepute.
- Pupils must not take, use, share, publish or distribute images of others.
- 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.

3.5 Dunclug College Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.The following should be read in conjunction with the **Dunclug College Data Protection Policy**.

Dunclug College:

- will hold only 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. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for.
- provides staff, parents, volunteers, teenagers and older children with information about how the college looks after their data and what their rights are in a clear Privacy Notice
- staff receive data protection training at induction and appropriate refresher training thereafter.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any college personal data to personal devices except in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

4.0 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table lists some of the technologies Dunclug College has identified as having benefits:

Communication Technologies	Staff	Pupils
Use of mobile phones in lessons	If necessary	With Permission
Use of mobile phones in social time	Permitted	Permitted
Taking photos on mobile phones/cameras	Permitted	With permission
Use of personal email addresses on C2k system	Permitted	Permitted
Use of Dunclug College email for personal emails	Not permitted	
Use of social media & blogs	Permitted	

When using communication technologies, Dunclug College considers the following as good practice:

- C2k email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the C2k email service to communicate with others when in school, or on C2k systems working remotely.
- Users report to the SLT receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond online.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to communicate appropriately when using digital technologies.
- Only C2k email addresses should be used to email members of staff.

Social Media Use: Dunclug College provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training including: acceptable use; social media risks; checking of settings; data protection.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made on social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating the school community
- Personal opinions should not be attributed to Dunclug College.
- Security settings on personal social media profiles are checked

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with Dunclug College or impacts on Dunclug College, it must be made clear that the member of staff is not communicating on behalf of the college with an appropriate disclaimer.
- Personal communications which do not refer to the school are outside this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school.
- The school does not respond to social media comments via social media

5.0 Appendices

5.1 Pupil Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *Dunclug College* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will not disclose or share personal information about myself or others on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Dunclug College systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not use the Dunclug College systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission from a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I will not damage or remove data belonging to others

I recognise that the school has a responsibility to maintain the security and integrity of the technology:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- When I am using the internet to find information, I should take care to check that the information that I access is accurate

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community.
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include) loss of access to the school network, detentions, suspensions, contact with parents and the event of illegal activities involving the police.

Student/Pupil Acceptable Use Agreement Form

I have read and understand the *Dunclug College Pupil Acceptable Use Agreement,* which is available on the school website, and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I am involved in completing school work using school based electronic platforms and communicating with staff and other students, both inside and outside school.
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school.
- I understand that the C2k system in school is a monitored system.
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include) loss of access to the school network, detentions, suspensions, contact with parents and the event of illegal activities involving the police.

Name of Student/Pupil: _____ Registration Class: _____

Signed: _____ Date: _____

Parent/Carer Countersignature: _____

5.2 Parent/Carer Acceptable Use Agreement

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users. A copy of the *pupil* acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.
Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name: _____ Pupil Name: _____

- I have read Dunclug College Online Safety Policy and associated Acceptable Use Policies, which are available on the school website.
- As the parent/carer of the above *pupils*, I give permission for my son/daughter to have access to the internet and to ICT systems at school.
- *I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.*
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: _____

Date: _____

5.3 Use of Digital/Video Images

- The use of digital/video images plays an important part in learning activities. Staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.
- Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.
- The school will comply with the Data Protection Act and request parent's/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.
- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *pupils* in the digital/video images.
- Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Digital/Video Images Permission Form

Parent/Carers Name:_____ Pupil Name:_____

As the parent/carer of the above student/pupil, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities.	Yes/No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No
Insert statements here that explicitly detail where images are published by the school/academy	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed: _____ _____

Date: _____ _____

5.4 Staff (and Volunteer) Acceptable Use Policy

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications when using systems:

- I will not copy, remove or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with pupils and parents/carers.
- I will not engage in on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of Dunclug College:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school site:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school digital technology systems within these guidelines.

Staff/Volunteer Name: _____ _____

Signed: _____ _____

Date: _____ _____

5.5 School Technical Security Policy

- College technical systems will be managed in accordance with guidance from C2k.
- there will be regular reviews of the safety and security of school technical systems
- servers, wireless systems and cabling must be securely located
- 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/academy systems and data
- all users will have clearly defined access rights to school technical systems.
- 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
- Remote management tools are used to control workstations and view users activity
- personal data cannot be sent over the internet or taken off the college site unless safely encrypted or otherwise secured.

Password Security

- Dunclug College networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school/academy technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and students/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 breach of security.
- Passwords must not be shared with anyone.

Password requirements:

- Passwords must be eight characters long.
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system

Notes for C2K Managers

- Each C2K manager should have an individual account.
- There must always be at least two C2k managers nominated by the Principal

Filtering

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- Dunclug College maintains and supports the managed filtering service provided by the C2K.
- The school has provided enhanced/differentiated user-level filtering through the use of the C2k filtering programme.

- Mobile devices that access the school internet connection will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the C2k. If the request is agreed, this action will be recorded.

Education/Training/Awareness

Staff & Student Users will be made aware of the filtering systems through:

- the Acceptable Use Policy
- Induction training
- staff meetings, briefings, Inservice

Parents will be informed of the school's filtering policy through the acceptable use agreement and through the college website.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the acceptable use agreement.

5.6 Dunclug College BYOD Policy

Dunclug College has provided technical solutions for the safe use of mobile technology for school devices and personal devices:

- Appropriate access control is applied to all mobile devices according to the requirements of the user
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- All school devices are subject to routine monitoring
- Pro-active monitoring has been implemented to monitor activity

When personal devices are permitted:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school
- Dunclug College accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- The school recommends that personal devices are made easily identifiable.
- Dunclug College is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- Devices may not be used in tests or exams
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for protecting and looking after their device in school.
- Personal devices should be charged before being brought to the Dunclug College as the charging of personal devices is not permitted during the school day
- Devices must be in silent mode on the school site.
- School devices are provided to support learning.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc...) that would stop the device working as it was originally set up and intended to work is not permitted
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity.
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances

5.7 Social Media Policy

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school/academy.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Dunclug College respects privacy and understands that staff and pupils may use social media forums in their private lives.
- All professional communications are within the scope of this policy.
- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the Dunclug College are outside the scope of this policy.
- Digital communications with pupils/students are also considered. Staff may use social media to communicate with learners via a school/academy social media account for teaching and learning purposes.

Process for creating new accounts

The Dunclug College community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present their case to the SLT covering the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected.

Monitoring

School accounts must be monitored regularly and frequently. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school/academy social media account.

Behaviour

- Dunclug College requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school..
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely

seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policy
- Dunclug College will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school/academy users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload pupil pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school/academy social media accounts. Pupils should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

Personal use of Social Media

- Staff
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school/academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Pupil
    - Staff are not permitted to follow or engage with current pupils of the school on any personal social media network account.

    - The school's education programme should enable the pupils to be safe and responsible users of social media.
    - Pupils are encouraged to comment or post appropriately about the school.
- Parents/Carers
    - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
    - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school/academy.
- The school/academy should effectively respond to social media comments made by others according to a defined policy or process.

Managing your personal use of Social Media

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint and keep your personal information private
- When posting online consider; Scale, Audience and Permanency of what you post
- Know how to report a problem

Acknowledgements

Produced from template supplied by South West Learning Grid