1 Policy Aim

This policy makes clear the principles which both staff and students are expected to adhere to when using social networking sites. It is a policy that should be read in conjunction with supporting documentation, for which hyperlinks are attached.

The intention of this policy is not to stop Darlington College employees or students from conducting legitimate activities on the internet, nor to stifle constructive criticism, but serves to highlight those areas in which problems can arise for both individual employees and the organisation.

Digital technologies have become integral to the lives of children and young people, both within Colleges and outside College. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

2 Scope of Policy

This policy applies to all members of the College community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of College ICT systems, both in and out of the College.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the College, but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Discipline Procedure.

The College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of College.

2.1 Keeping Children Safe in Education, Sept 2021 states:

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

3 Background

Social media is the term commonly used for websites which allow people to interact with each other in some way - by sharing information, opinions, knowledge and interests. As the name suggests, social media involved the building of online communities or networks, encouraging participation and engagement.

Social networking websites are perhaps the most well-known examples of social media, but the term covers other web-based services. Examples include Blogs, audio and video podcasts, Wiki's, message boards, social bookmarking websites, photo, document and video content sharing websites or micro-blogging services.

These media provide a number of benefits in which employees may wish to participate in their personal life. However, when an individual clearly identifies their employment with Darlington College and/or discusses their work which may involve other partners such as Teesside University (in the case of higher education provision) of individual Schools (in the case of pre-16 provision), they are expected to behave appropriately, and in ways that are consistent with the organisation's values and policies.

For the purposes of this policy, "students" refers to all individuals who learn through provision provided by the college, including higher education students and pre-16 students on school rolls.

4 Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the College:

4.1 Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body (usually the Safeguarding Board Member) will take on the role of the Online Safety Governor and will liaise with the College Safeguarding Team on any relevant

issues around online safety.

4.2 **Executive Team:**

- The Executive Team has a duty of care for ensuring the safety (including online safety) of members of the College community, though the day to day responsibility for online safety will be delegated to the Safeguarding Manager and the IT Manager.
- The Principal and (at least) another member of the Executive Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal / Executive Team are responsible for ensuring that the Safeguarding Team and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal and Executive Team will ensure that there is a system in place to allow for monitoring and support of those in College who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Executive Team will receive regular monitoring reports from Safeguarding Manager/IT Manager.

4.3 **Safeguarding Manager will:**

- Take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the College online safety policies / documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provide training and advice for staff
- Liaise with the Local Authority / relevant body
- Liaise with College technical staff
- Receive reports of online safety incidents and follow these up with the support of the Safeguarding and Transitions Officer and the Student Support Team
- Report regularly to Deputy Principal.

4.4 **The IT Manager / Technical Staff will:**

- Ensure that the College's technical infrastructure is secure and is not open to misuse or malicious attack
- that the *College* meets required online safety technical requirements and any Local Authority other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- 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 *network / internet / Learning Platform / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the Safeguarding Manager for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in College policies

4.5 **Teaching and Support Staff will:**

- Not reveal confidential information or comment about students, stakeholders or anyone associated to the organisation.
- Not engage in activities on the internet which might bring the college into disrepute.
- Act in a transparent manner when altering online sources of information such as websites like Wikipedia.
- Not use the internet in any way to attack or abuse colleagues.
- Not post defamatory, derogatory or offensive comments on the internet about colleagues, students, their work or the college.

Any online activities associated with work for the organisation should be discussed and approved in advance by a line manager and in conjunction with the Marketing and Engagement Manager.

All employees of the college should be mindful of the personal information they disclose on social networking sites, especially with regards to identity theft. Making information such as your date of birth, your place of work and other personal information publically available can be high risk in terms of identity theft.

Employees of the college should also act in a manner which does not bring the organisation into disrepute. This applies to both open and private sections of a site if you are identifying yourself as an employee of Darlington College.

If an employee is contacted by the media about posts they have made on a social networking site that relate to the college they should talk to their manager before responding. The Marketing and Engagement Manager must also be consulted.

Social networking sites allow photographs, videos and comments to be shared with thousands of other users. However, it may not be appropriate to share work-related information in this way. For example, there may be an expectation that photographs

taken at a private college event will not appear publically on the internet, both from those present and perhaps those not at the event.

Employees should be considerate to their colleagues in such circumstances and should not post information when they have been asked not to. They should also remove information about a colleague if that colleague asks them to do so.

Under no circumstances should offensive comments be made about Darlington College, colleagues, the college's business or stakeholders on the internet. This may amount to cyber-bullying and will be deemed a disciplinary offense.

Personal blogs and websites should not reveal confidential information about students, employees or the organisation. This may include aspects of Darlington College's policy, plans or details of internal discussions. If in doubt about what might be confidential, employees should consult their line manager.

Blogs or websites which do not identify the blogger as an employee of Darlington College, do not discuss the organisation and are purely about personal matters would normally fall outside this policy.

Employees who already have a personal blog or website which indicates in any way that they work for Darlington College, should discuss any potential conflicts of interest with their line manager.

Similarly, employees who want to start blogging and wish to say that they work for the college should discuss any potential conflicts of interest with their line manager.

If a blog makes it clear that the author works Darlington College, it should include a simple and visible disclaimer such as, "These are my personal views and are not those of Darlington College". The college's logo or professional photographs must not be used on personal web pages.

Personal blogs and websites should not be used to attack or abuse colleagues, stakeholders or students. Staff members should respect the privacy and feelings of others. Remember also that if you break the law on a blog (for example by posting something defamatory or infringing copyright), you will be personally responsible.

If an employee thinks something on their blog or website gives rise to concerns about a conflict of interest, and in particular concerns about impartiality or confidentiality, this must be discussed with their line manager.

If an employee is offered payment to produce a blog for a third party this could constitute a conflict of interest and must be discussed with the Principal.

If an employee is contacted about posts on their blog that relate to the firm they should talk to their line manager before responding. The Communications Manager should also be consulted.

Any misuse of this Policy will result in disciplinary procedures up to and including dismissal

Staff should also ensure that they:

- They have an up to date awareness of online safety matters and of the current College Online Safety Policy and practices
- They have read and understood Staff Code of Conduct
- They report any suspected misuse or problem to the HR Manager or Safeguarding Manager for investigation / action / sanction
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official College systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the Online Safety Policy and acceptable use policies eg ICT Code of Conduct
- Students have a good understanding of 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 College activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned students 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.
- When creating a Google Classroom you must invite, as a minimum, one other member of staff and the appropriate "ssaXadmin@darlington.ac.uk" dummy account, where X is the appropriate subject sector area identifier.

4.6 **The Safeguarding Team will:**

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
- cyber-bullying

It is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

The Safeguarding Team will discuss issues arising from online safety in their termly Safeguarding Strategy meetings and will monitor:

- The production / review / monitoring of the College Online Safety Policy / documents.
- Monitoring network / internet / incidents
- Ensuring that staff and the students are fully aware and up to date about the online safety provision.

4.7 **Students:**

- Are responsible for using the College digital technology systems in accordance with the ICT Code of Conduct and Student Code of Conduct
- 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 and know how to do so
- Will be expected to know and understand 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 cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of College and realise that the College's Online Safety Policy covers their actions out of College, if related to their membership of the College.

4.8 **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. The College will take every opportunity to help parents understand these issues through parents' evenings, newsletters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the College in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at College events
- Access to parents' sections of the website and on-line student records
- Their son/daughter's personal devices in the College (where this is applicable)

5 Education

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

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum will be provided as part of group tutorials and as an integral part of learning sessions
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. They should be made aware of the Prevent Strategy and the College's actions around this
- Students should be helped to understand the need for the student ICT Code of Conduct and Student Code of Conduct
- 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 students 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 students 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, students may need to research topics (eg 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.

5.1 Education – Parents and Carers

Many parents and carers have only a limited understanding of online 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.

The College will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions

- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications (see table at end of policy)

5.2 Education and Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All staff must have mandatory safeguarding training at the start of their employment with the College and this will be refreshed every 3 years.
- It is expected that some staff will identify online safety as a training need within the performance appraisal process.
- The Safeguarding Manager will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations and cascade this to teams.

5.2 Training – Governors

- Governors will receive mandatory safeguarding training which will include updates on online safety
- They will approve and be familiar with the Online Safety Policy
- The Safeguarding Manager will update them with any necessary information or changes to Keeping Children Safe in Education

6 Technical – infrastructure / equipment, filtering and monitoring

The College IT team will be responsible for ensuring that the College 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 relevant people named in the above sections will be effective in carrying out their online safety responsibilities

- College technical systems will be managed in ways that ensure that the College meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of College 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 their username and password and will be required to change their password when prompted to do so

- The “master / administrator” passwords for the College ICT system, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (eg College safe)
- The IT Manager is 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
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. 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
- Internet filtering should ensure that students are safe from terrorist and extremist material when accessing the internet. The College is clear on its responsibilities on this by following the Prevent Duty.
- The College has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / students etc)
- College technical staff regularly monitor and record the activity of users on the College technical systems and users are made aware of this in the ICT Code of Conduct
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. This would be the IC Dept for staff and students would report issues to their Tutor.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the College systems and data. These are tested regularly. The College infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the College systems.
- An agreed policy is in place that allows staff to / forbids staff from downloading utube files and installing programmes on College devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on College devices. Personal data cannot be sent over the internet or taken off the College site unless safely encrypted or otherwise secured.

7 Mobile Technologies

Mobile technology devices may be College owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the College’s wireless network. The device then has access to the wider internet which may include the College’s learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a College context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant College polices including but not limited to the Safeguarding

Policy, Discipline Procedure, Bullying Policy, ICT Code of Conduct and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the College's Online Safety education programme.

8 Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever 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 College 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 students 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 eg on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the College website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their 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 students 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 College equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Students' work can only be published with the permission of the student and parents or carers.

9 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the College considers the following as good practice:

- The official College email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the College email service to communicate with others when in College, or on College systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the College 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 students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) College systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used, and students will be provided with individual College email addresses for educational use.
- Students / 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 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 College website and only official email addresses should be used to identify members of staff.

10 Social Media – Protecting Professional Identity

All Colleges have a duty of care to provide a safe learning environment for students and staff. Colleges could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the College liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The College provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the College through:

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

10.1 **College staff should ensure that:**

- No reference should be made in social media to students, parents / carers or College staff
- They do not engage in online discussion on personal matters relating to members of the College community
- Personal opinions should not be attributed to the College or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

10.2 **When official College social media accounts are established there should be:**

- A process for approval by the Marketing and Engagement Manager
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under College disciplinary procedures.

10.3 **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 the College or impacts on the College it must be made clear that the member of staff is not communicating on behalf of the College 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 College are outside the scope of this policy
- Where excessive personal use of social media in College is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The College permits reasonable and appropriate access to private social media sites.

10.3 **Monitoring of Public Social Media:**

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

- The College's use of social media for professional purposes will be checked regularly by the Marketing and Engagement Manager to ensure compliance with the College policies.

10.4 **Responding to Incidents of Misuse:**

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities:

10.5 **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, this must be reported to the Safeguarding Manager immediately who will inform the police.

10.6 **Other Incidents**

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

10.7 **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. Initially this should be reported to the HR Manager who will begin an investigation.
- 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 record (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the HR Manager or other senior Manager 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 the Designated Officer in the Local Authority
  - 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
- promotion of terrorism or extremism
- 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 College and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed record should be retained by HR for evidence and reference purposes.

11 College Actions and Sanctions

It is more likely that the College 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 College 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.

12 Personal Safety Online

The promotion of professional and safe practice is a key priority for the College. Therefore, the following points noted below are deemed to help both staff and students make good decisions about protecting and safeguarding themselves and others:

- be familiar with privacy options on social networking sites
- be familiar with Ashley's Rules
- set appropriate privacy guards for your personal comfort level
- be aware that no privacy option protects you 100% from personal information being shared beyond desired boundaries
- be aware that information posted on-line may be perceived differently depending on the viewer, despite the intended effect or outcome
- inappropriate incidents reported to the college will be investigated and dealt with through the college's disciplinary procedures or, in some cases, may require a criminal investigation

12.1 If a member of staff is ever contacted by the press about information that has been posted to their social networking site and links them to Darlington College, then the College's Marketing Manager must be informed. Similarly, if a student of the college is contacted by the press concerning posts on their social networking which relates them to the college, then he/she should inform their professional tutor who, in turn, will contact the college's Marketing Manager.

12.2 The College is responsible for managing its own social networking sites. It has a procedure which outlines clearly who can set up sites, how sites are recorded and monitored, circumstances under which any posts or comments can be removed and arrangements to gain permission for using the college logo. Support and development is delivered through staff induction and mandatory CPD, and for students through the induction process.

12.3 If you are using a Social Network for academic reasons or for marketing reasons then you are to inform the marketing team of this. You are also required to add a designated member of the marketing team as an administrator on your site, if the Social Network allows this (for example in Facebook pages and groups). The marketing team will keep a central record of all approved Social Networking activities operating on behalf of the College. The user is responsible for managing the activity on this Social Networking site and is responsible for adhering to the procedures outlined in this document.

13 Photographic or Video Images

If an external organisation asks to come into the College to photograph or film the College premises, staff and/or students then advance notice must be given. This notice should indicate clear dates and times, a description of the areas that are to be accessed and the purpose of activity. This notification must be given to the Marketing and Engagement Manager using the College's consent form where appropriate and they will grant permission if they see fit.

The Marketing and Engagement Manager will then:

- Liaise with any relevant staff ie Safeguarding team
- Communicate with the external organisation with regards to the shoot
- Accompany (or delegate to a member of the team to accompany) the external organisation throughout the shoot
- Gain verbal confirmation from students that they are happy to be filmed/ photographed/recorded where there is a large group of students
- Will ask students to complete an audio/photographic/video image consent form for small groups of students or individuals.

13.1 **Recording by students or staff**

Students and staff must seek consent of other students before recording any audio/ photographic/video images of other students in the College. Users should understand that if they publicly post any content it becomes the sole responsibility of the individual who originally posted the content.
Darlington College will not be liable, under any circumstances for any errors, omissions, loss or damages of any kind incurred as a result of use of any content posted on any social media sites or in the public domain. Students and staff are required to protect confidential and proprietary information regarding Darlington College, staff members or students.

SUPPORT FOR STAFF, STUDENTS and PARENTS/CARERS

Organisation/Resource	What it does/provides
www.thinkuknow.co.uk	NCA CEOPs advice on online safety
www.disrespectnobody.co.uk	Home Office advice on healthy relationships, including sexting pornography
https://www.saferinternet.org.uk/	Contains a specialist helpline for UK schools and colleges
https://www.internetmatters.org/	Help for parents on how to keep their children safe online
https://www.childnet.com/parents-and-carers/hot-topics/cyberbullying	Guidance for schools on cyberbullying
https://educateagainsthate.com/	Practical advice for parents, teachers and governors on protect children from extremism and radicalisation.
https://www.gov.uk/government/groups/council-for-child-internet-safety-ukccis	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
https://www.nspcc.org.uk/	NSPCC advice for schools and colleges

Hyperlinks to College procedures and policies*:*

Safeguarding Policy
http://staffnet/Executive Team/College%20Policies/15%20-%20Safeguarding%20Policy%20-%20approved%2023.10.18.pdf

Information Security Management Policy
http://staffnet/Executive Team/College%20Policies/32%20-

%20Information%20Security%20Management%20Policy%20and%20Code%20of%20Practice%20for%20Users%20-%20approved%20April%202018.pdf%20Information%20Security%20Management%20Policy%20and%20Code%20of%20Practice%20for%20Users%20-%20approved%20April%202018.pdf

The Corporation of Darlington College actively supports and promotes equality and diversity in all matters relating to education and employment. Consequently the Corporation aims to identify and eliminate attitudes, practices and procedures which discriminate against people on grounds of age, gender, race, sexual orientation, disability, religion/belief, gender re-assignment, social background, marital status, nationality/citizenship or any personal characteristic of the individual(s) and where the actions or comments of another person(s) are viewed as demeaning and unacceptable to the recipient.

a. CPD is available to support staff to manage difficult situations.

b. The Deputy Principal will monitor this Policy and will provide regular reports and recommendations to the Executive Teamutive and Corporation Board as appropriate.

Approval

Signed:

Kate Roe Date:
(Principal and Chief Executive)

Endorsed by the College Corporation
Signed:

Mr Calvin Kipling Date:
(Chairman)

APPENDIX 1

Audio, Photographic and Video Image Consent Form

In signing this form I give Darlington College permission to take my photographic and/or video image, record audio of me talking whilst attending Darlington College sites, courses or any other related event and to display it in education or publicity material. Such material may include but not exclusively the College website, electronic formats, printed publications, display stands, posters and College social media sites.

In participating in this material: a visitor I agree to waive any performing rights; as a student or staff member of the College, this also includes intellectual property rights of the material recorded.

Event/Activity/Project Title: ……

Date and time of Event: ……

Event Organiser: ……

Photographer: ……

Recordist Names/ Contact Details: ……

<u>Your Agreement</u>

Print Name: …… Signature: ……

Contact Details: ……

Date: ……

I am associated with Darlington College, as a staff member/student/visitor (please circle as appropriate)

Course: ……

Staff Name/Student Name/Number: ……

Telephone Number: ……

The information provided in this form is managed and stored in accordance with GDPR

Marketing Department, Darlington College, Central Park, Haughton Road, Darlington, County Durham, DL1 1DR