ASKHAM BRYAN COLLEGE

E-Policy
RE16

Equality Impact Assessment: Askham Bryan College recognises the importance of the Equality Act 2010 and its duties under the Act. This document has been assessed to ensure that it does not adversely affect staff, students or stakeholders on the grounds of any protected characteristics.

Contents

Version: August 2018	Next Review: December 2019	Author: Director of Student Services	SMT Owner: Director of Student Services

1. PURPOSE

1.1. The purpose of this e-safety policy is to:

- Safeguard and protect all members of Askham Bryan College ('The College') community online;
- Identify approaches to educate and raise awareness of e-safety throughout the community;
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology; and
- Identify clear procedures to use when responding to e-safety concerns.

1.2. The College identifies that the issues classified within e-safety are considerable, but can be broadly categorised into three areas of risk:*

- **Content:** being exposed to illegal, inappropriate or harmful material;
- **Contact:** being subjected to harmful online interaction with other users; and/or
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

(*for example: Access to illegal, harmful or inappropriate images or other content; Unauthorised access to / loss of / sharing of personal information; The risk of being subject to grooming by those with whom they make contact on the internet; The sharing / distribution of personal images without an individual's consent or knowledge; Inappropriate communication / contact with others, including strangers; Cyber-bullying; Access to unsuitable video / internet games; An inability to evaluate the quality, accuracy and relevance of information on the internet; Plagiarism and copyright infringement; Illegal downloading of music or video files; The potential for excessive use which may impact on the social and emotional development and learning of the young person).

1.3. The policy takes into account the following DfE guidance:

- 'Keeping Children Safe in Education' September 2018;
- 'Preventing and tackling bullying: Advice for headteachers, staff and governing bodies' July 2017; and
- 'Sexual violence and sexual harassment between children in schools and Colleges: Advice for governing bodies, proprietors, headteachers, principals, senior leadership teams and designated safeguarding leads' December 2017.

2. POLICY SCOPE

2.1. The College believes that e-safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online. The College identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. The College believes that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.

2.2. This policy applies to all staff including the governing body, teaching staff, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the College (collectively referred to as 'staff' in this policy) as well as students and parents/carers.

2.3. This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with College issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.4. Links with other policies and practices

This policy links with a number of other policies, practices and action plans including:

- Bullying and Harassment policy
- Acceptable Use Policies (AUP) and/or the Staff and Student Codes of Conduct
- Behaviour Management and Disciplinary policy
- Safeguarding policy
- Data Protection Policy

3. MONITORING AND REVIEW

The College will review this policy at least annually. The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

- We will ensure that we regularly monitor internet use and evaluate e-safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of e-safety, the Designated Safeguarding Lead will be informed of e-safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on e-safety incidents, including outcomes.
- Any issues identified will be incorporated into the College self-assessment processes.

4. ROLES AND RESPONSIBILITIES

- The College has nominated the Senior Designated Safeguarding Officer to be the e-safety lead.
- The College recognises that all members of the community have important roles and responsibilities to play with regards to e-safety.

4.1. The leadership and management team will:

- Ensure that e-safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding e-safety; including a Code of conduct and/or an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of College systems and

networks.

- Ensure that e-safety is embedded within a progressive whole College curriculum, which enables all students to develop an age-appropriate understanding of e-safety.
- Support the Senior Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their e-safety responsibilities.
- Ensure there are robust reporting channels for the College community to access regarding e-safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate e-safety practice to identify strengths and areas for improvement.

4.2. The Senior Designated Safeguarding Officer (SDSO) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding e-safety and communicate this with the College community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate e-safety training.
- Work with staff to coordinate participation in local and national events to promote positive e- behaviour, such as Safer Internet Day.
- Ensure that e-safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of e-safety concerns, as well as actions taken, as part of the College's safeguarding recording mechanisms.
- Monitor e-safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report e-safety concerns, as appropriate, to the management team and Corporation.
- Work with the leadership team to review and update e-safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and/or e-safety.

4.3. It is the responsibility of all members of staff to:

- Contribute to the development of e-safety policies.
- Read and adhere to the e-safety policy and AUPs.
- Take responsibility for the security of College systems and the data they use, or to which they have access.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed e-safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of e-safety issues and how they may be experienced by the learners in their care.
- Identify e-safety concerns and take appropriate action by following the College's safeguarding policies and procedures.
- Know when and how to escalate e-safety issues, including signposting to appropriate support, internally and externally.

- Take personal responsibility for professional development in this area.

4.4. It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the SDSO and leadership team, especially in the development and implementation of appropriate e-safety policies and procedures.
- Implement appropriate security measures (including password policies and encryption) to ensure that the College's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Report any filtering breaches to the SDSO and leadership team, as well as, the College's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the SDSO, in accordance with the College's safeguarding procedures.

4.5. It is the responsibility of students (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate e-safety education opportunities.
- Contribute to the development of e-safety policies.
- Read and adhere to the College AUPs.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing e-safety issues.

4.6. It is the responsibility of parents and carers to:

- Read the College AUPs and encourage their children to adhere to them.
- Support the College in their e-safety approaches by discussing e-safety issues with their children and reinforce appropriate, safe e- behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the College's homeworking agreement and/or AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the College, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the College e-safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. EDUCATION AND ENGAGEMENT APPROACHES

5.1. Education and engagement with students

The College will establish and embed a progressive e-safety curriculum throughout the whole College, to raise awareness and promote safe and responsible internet use amongst students by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including e-safety in programmes of study, covering use both at home and College.
- Reinforcing e-safety messages whenever technology or the internet is in use.
- Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The College will support students to read and understand the AUP in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology by students.
- Implementing appropriate peer education approaches.
- Seeking student voice when writing and developing College e-safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support the Colleges internal e-safety education approaches.

5.2. Vulnerable Students

- The College is aware that some students are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The College will ensure that differentiated and ability appropriate e-safety education, access and support is provided to vulnerable students.
- The College will seek input from specialist staff as appropriate, including the Learning Support Manager.

5.3. Training and engagement with staff

The College will:

- Provide and discuss the e-safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate e-safety training for all staff on a regular basis, with at least annual updates, as part of existing safeguarding training / updates. (This will cover the potential risks posed to students (Content, Contact and Conduct) as well as professional practice expectations).
- Make staff aware that College systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with College's policies when accessing College systems and devices.
- Make staff aware that their online conduct out of College, including personal use of social media, could have an impact on their professional role and reputation within College.

- Highlight useful educational resources and tools which staff should use, according to the age and ability of the students.
- Ensure all members of staff are aware of the procedures to follow regarding e-safety concerns affecting students, colleagues or other members of the College community.

5.4. Awareness and engagement with parents and carers

The College recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.

The College will build a partnership approach to e-safety with parents and carers by:

- Providing information and guidance on e-safety in a variety of formats. This will include offering specific e-safety awareness information and highlighting e-safety at other events such as parent evenings and open days.
- Drawing their attention to the College e-safety policy and expectations in any newsletters, letters, the prospectus and on the College website.
- Requesting that they read the College AUP and discuss its implications with their children.

6. REDUCING E-RISKS

The College recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in College is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a College computer or device.

All members of the College community are made aware of the College's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the College's AUP and highlighted through a variety of education and training approaches.

7. SAFER USE OF TECHNOLOGY

7.1. Classroom Use

The College uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet, which may include search engines and educational websites
- College Moodle
- Email

- Digital cameras, web cams and video cameras

- All College owned devices will be used in accordance with the College's AUP
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The College will ensure that the use of internet-derived materials, by staff and students, complies with copyright law and acknowledge the source of information.
- Supervision of students will be appropriate to their ability.
- Students' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved e- materials, which supports the learning outcomes planned for the students' ability.
- 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 Head of IT 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.
- Students in residential provision: The College will balance a student's ability to take part in appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by students in accordance with the national minimum standards (NMS).

7.2. Managing Internet Access

- The College will maintain a written record of users who are granted access to the College's devices and systems.
- All staff, students and visitors will read and sign an AUP before being given access to the College computer system, IT resources or internet.

7.3. Filtering and Monitoring

7.3.1. Decision Making

- The College governors and leaders have ensured that the College has appropriate filtering and monitoring in place, to limit student's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what students can be taught, with regards to e- activities and safeguarding.
- The College's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our College's specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

7.3.2. Filtering

- The College uses Websense which blocks sites based on categories such as: pornography, racial hatred, extremism, gaming and sites of an illegal nature etc. The College filtering system includes sites on the Internet Watch Foundation (IWF) list.

7.3.3. Dealing with Filtering breaches

- The College has a clear procedure for reporting filtering breaches.
    - If students discover unsuitable sites, they will be required to turn off the monitor/screen and report the concern immediate to a member of staff. The member of staff will report the concern (including the URL of the site if possible) to the Senior Designated Safeguarding Officer and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.

- Any material that the College believes is illegal will be reported immediately to the appropriate agencies, such as: Internet Watch Foundation, CEOP (Child Exploitation and Online Protection) and / or the police.

7.3.4. Monitoring

- The College will appropriately monitor internet use on all College owned or provided internet enabled devices. This is achieved by: firewall generated logs being used to generate reports on set categories
- The College has a clear procedure for responding to concerns identified via monitoring approaches. Reports are automatically sent to the SDSO based on the set categories
- All users will be informed that use of College systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4. Managing Personal Data Online

7.4.1. Data Protection

Personal data will only be processed in a manner that complies with the General Data Protection Regulation ("GDPR"), the Data Protection Act 2018 (subject to Royal Assent) and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable, the guidance and codes of practice issued by the Information Commissioner.

GDPR provides that personal data must be:

1. processed lawfully, fairly and in a transparent manner;

2. collected for specified, explicit and legitimate purposes only;

3. adequate, relevant and limited to what is necessary for the purposes of that processing activity;

4. accurate and where necessary, kept up to date;

5. retained only for as long as is necessary for the purposes of the processing; and

6. processed securely and in an appropriate manner to maintain security**.**

Personal data provided by a student or staff member will be stored and processed by the College, in the case of students, to support the enrolment of students and provision of education, and for various administrative purposes, for instance, monitoring of student loans, scholarships, payroll, attendance, examination/attainment, accommodation, marketing and event management. Any personal data will be securely destroyed after it is no longer required for these purposes. If a student is under 18 years of age, the College reserves the right to disclose information to the parent, guardian or carer, in appropriate circumstances.

In some instances, the College will share personal data with some third parties, including the Education and Skills Funding Agency (ESFA) and Department for Education (DfE) and with catering companies, transport companies and examination boards.

Where the College does this, there will be a clear purpose for the sharing, such as to ensure the provision of these services to staff and students, and in the case of the DfE and or ESFA, because the College is under a statutory obligation to share information with those organisations. The College will ensure that a contract/data sharing agreement is in place before any sharing takes place, to define expectations for the use and control of the data, to safeguard against any unauthorised use or loss of the same.

Personal data will be held in accordance with the College's data retention policy. This will be necessary for the purpose(s) for which that data was collected it, and after that time, the data will either be deleted or anonymised. All data will remain at all times within the UK and European Economic Area ("EEA").

An organisation must be able to demonstrate compliance with these principles to the UK's Supervising Authority, the Information Commissioner's Office ("ICO"), which has the power to punish organisations who fail to do so; in extreme cases by way of a financial penalty equivalent to €20 million or 4% of that organisation's annual turnover, whichever is the greater.

Staff must therefore ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;

- use personal data 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; and

- at all times adhere to the College's policies and procedures on data protection.

For further information, see the College's data protection policies which are available at https://able.askham-bryan.ac.uk/staff/course/view.php?id=187

7.4.2. Data Protection Officer

The College Senior Management Team has overall responsibility for ensuring compliance with data protection legislation and this policy and has appointed a Data Protection Officer, who is the Clerk to the Corporation. The Data Protection Officer will lead on the College's overall approach to data protection, assisted, where necessary, by the Legal and Compliance Adviser.

Any person who considers that this policy has not been followed should raise the matter with the Data Protection Officer by contacting judith.clapham@askham-bryan.ac.uk or by emailing DataProtection@askham-bryan.ac.uk .

Any person who is not satisfied with that response may then wish to contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

7.5. Security and Management of Information Systems

The College takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices
- The appropriate use of user logins and passwords to access the College network.
- Specific user logins and passwords will be enforced for all users.
- All users are expected to log off or lock their screens/devices if systems are unattended.

7.6. Password policy

- All members of staff will have their own unique username and private passwords to access College systems; members of staff are responsible for keeping their password private.
- All students are provided with their own unique username and private passwords to access College systems; students are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system.
    - Change their passwords every 90 days
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.

7.7. Managing the Safety of the College Website

- The College will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The College will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or students' personal information will not be published on our website; the contact details on the website will be the College address, email and telephone number.
- The administrator account for the College website will be secured with an appropriately strong password.
- The College will post appropriate information about safeguarding, including e-safety, on the College website for members of the community.

7.8. Publishing Images and Videos Online

- The College will ensure that all images and videos shared online are used in accordance with the associated polices: Acceptable Use Policy ;Staff Code of Conduct
- 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 e.g. on social networking sites.
- Staff 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.
- 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.
- For students under 18 years old, written permission from parents or carers will be obtained before photographs of students are published on the college website (but not the VLE).
- Student's work can only be published with the permission of the student and parents or carers if under 18.

7.9. Managing Email

- Access to College email systems will always take place in accordance with Data Protection legislation and in line with other College policies, including: Confidentiality, AUPs and Code of conduct.

    - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

- College email addresses and other official contact details will not be used for setting up personal social media accounts.

- Members of the College community will immediately tell the Senior Designated safeguarding Officer if they receive offensive communication, and this will be recorded in the College safeguarding files/records.
- The College will have a dedicated system for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

7.9.1. Staff usage

- The use of personal email addresses by staff for any official College business is not permitted. All members of staff are provided with a specific College email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and students and parents.

7.9.2. Student usage

- Students will use College provided email accounts for educational purposes.
- Students will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the College

7.10. Educational use of Video Conferencing and/or Webcams

The College recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.

- Videoconferencing contact details will not be posted publicly.
- College videoconferencing equipment will not be taken off College premises without prior permission from the SDSO.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away when not in use.

7.10.1. Users

- Parents and carers consent will be obtained prior to students taking part in video conferencing activities.
- Students will ask permission from a tutor before making or answering a videoconference call or message.
- Video conferencing will be supervised appropriately, according to the students' ability.

- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to video conferencing administration areas or remote control pages.

7.10.2. Content

- When recording a video conference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, the College will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The College will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-College site, staff will check that the material they are delivering is appropriate for the class.

7.11. Management of Learning Platforms

- The College uses Moodle as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, students and parents will have access to the LP.
- When staff and/or students' leave the College, their account or rights to specific College areas will be disabled.
- Students, staff and parents will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:

    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement. A student's parent/carer may be informed.
    - If the content is considered to be illegal, then the College will respond in line with existing child protection procedures.

- Students may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

7.12. Management of Applications (apps) used to Record Student Progress

- The College uses ProMonitor to track student progress and share appropriate information with parents and carers.
- The CEO is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation
- In order to safeguard students data:

    - Only College issued devices will be used for apps that record and store student's personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store student's personal details, attainment or images.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. SOCIAL MEDIA

8.1. Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The College community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; e- gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of The College community are expected to engage in social media in a positive, safe and responsible manner, at all times.

    - All members of The College community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

- The College will control student and staff access to social media whilst using College provided devices and systems on site.

    - Inappropriate or excessive use of social media during College/work hours or whilst using College devices may result in disciplinary or legal action and/or removal of internet facilities.

- Concerns regarding the online conduct of any member of the College community on social media, should be reported to the College and will be managed in accordance with our Anti-bullying, Behaviour and Safeguarding policies.

8.2. Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the College Code of conduct within the AUP.

8.2.1. Reputation

- All members of staff are advised that their e- conduct on social media can have an impact on their role and reputation within College. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

    - Setting the privacy levels of their personal sites as strictly as they can.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the College.

- Members of staff are encouraged not to identify themselves as employees of The College on their personal social networking accounts. This is to prevent information on these sites from being linked with the College and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post e- and to ensure that their social media use is compatible with their professional role and is in accordance with Colleges policies and the wider professional and legal framework:

    - Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.

- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the College.

8.2.2. Communicating with students, former students, parents, guardians and carers

- Staff should not add any current students or their parents, guardians and or carers onto their **personal** social media accounts (i.e. their social media accounts which they use to post information, updates, photos and/or provide comments about their lives outside the college).

- If a member of staff wishes to use social media as a way of contacting existing students, their parents' carers or guardians for the purposes of College business, please see section 8.5.2 below.
- Staff are strongly advised not to add any former students, their parents, guardians or carers onto their personal social media accounts.
- If a former student or family member is added to a personal social media account belonging to a member of staff, the staff member must not post anything onto that personal social media account which could compromises them or another staff member or bring the College into disrepute.

If a member of staff sees an inappropriate post on social media by a member of staff which could be seen by a student, former student, their parents, guardians or carers they must report it to the Designated Safeguarding Lead.

Staff may have contact with former students, their parents' carers or guardians on social media, provided that it is solely for professional (i.e. work or careers related) networking purposes.

8.2.3. Professional Networking

As a general principle staff should use their college contact details or a 'professional' profile for communication with current and prospective students, and ensure that any communication is both professional and necessary.

A professional profile is where a member of staff maintains an online presence explicitly for professional purposes. This profile should minimise any information which could be used to compromise the individual and should not be used to record social activity or personal opinion but may be used to record professional information or opinion. It is important that a professional profile is not added to non-professional networks or linked to the profiles of others except where the connection is professional. This might legitimately include links to student groups but would be unlikely to include groups of friends / family.

8.3. Students' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources.
- Any concerns regarding students' use of social media, both at home and at College, will be dealt with in accordance with existing College policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Students will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, College attended,

other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- To use safe passwords.
- To use social media sites which are appropriate for their age / abilities.
- How to block and report unwanted communications and report concerns both within College and externally.

8.4. Official Use of Social Media

8.4.1. The College official social media channels are:

- Facebook (ABC) www.facebook.com/askhambryancollege;
- Facebook (Wildlife Park) www.facebook.com/ABCWildlifePark;
- Facebook (Newton Rigg) www.facebook.com/NewtonRiggCollege;
- Twitter (ABC) www.twitter.com/askhambryan;
- Twitter (Newton Rigg) www.twitter.com/newtonrigg ;
- YouTube www.youtube.com/askhambryancollege
- Instagram www.instagram.com/askhambryancollege;
- LinkedIn (ABC)https://www.linkedin.com/company/askham-bryan-college/;
- LinkedIn (Newton Rigg)https://www.linkedin.com/showcase/newton-rigg-college/;
- LinkedIn (Wildlife Park) https://www.linkedin.com/showcase/askham-bryan-wildlife- and-conservation-park/.

8.4.2. The official use of social media sites, by the College, only takes place with clear educational or community engagement objectives, with specific intended outcomes.

- The official use of social media as a communication tool has been formally risk assessed and approved by the Designated Safeguarding Lead.
- Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.

8.4.3. Official College social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

- Staff use College provided email addresses to register for and manage any official College social media channels.
- Official social media sites are suitably protected and, where possible, run and/or linked to/from the College website.
- Public communications on behalf of the College will, where appropriate and possible, be read and agreed by at least one other colleague.

8.4.4. Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality and Safeguarding:

- All communication on official social media platforms will be clear, transparent and open to scrutiny.

8.4.5. Parents, carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

- Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Any official social media activity involving students will be moderated by the College where possible.

Parents and carers will be informed of any official social media use with students and written parental consent will be obtained, as required..

8.5. Expectations of staff use of College social media

8.5.1. Members of staff who follow and/or like the College social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

8.5.2. If members of staff are participating in e- social media activity as part of their capacity as an employee of the College, they will:

- Set up a **separate profile** on the social media platform to be used exclusively for work purposes i.e. for college business only, and will not use their own personal social media account.
- Be professional at all times and aware that they are an ambassador for the College.
- Ensure that the social media group is closed (i.e. only open to invited members) and that the privacy of the members is protected.
- Disclose their official role and/or position within the College.
- Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: Defamation, Confidentiality, Intellectual property, Data protection and Equalities laws.
- Ensure that they have appropriate consent before posting images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the College unless they are authorised to do so.
- Not engage with messaging with students, their parents, guardians or carers on any matters other than those strictly related to the students' education at the College.
- Inform their line manager, the Senior Designated Safeguarding Officer and/or the Designated Safeguarding Lead of any concerns, such as criticism, inappropriate content or contact from students.
- Ensure that the member of staff's Head of Department and or Director is a member of the social media group.

9. USE OF PERSONAL DEVICES AND MOBILE PHONES

The College recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within College.

9.1. Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate College policies, including, but not limited to: Anti-bullying, Behaviour and Safeguarding.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times:

    - All members of The College community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the College accepts no responsibility for the loss, theft or damage of such items on College premises.
    - All members of The College community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

- Mobile phones and personal devices are not permitted to be used in specific areas within the College site such as changing rooms, toilets. The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of The College community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the College Behaviour or Safeguarding policies.

9.2. Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant College policy and procedures.
- Staff will be advised to:

    - Keep mobile phones and personal devices in a safe and secure place during lesson time
    - Keep mobile phones and personal devices switched off or switched to ‘silent’ mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as ‘airdrop’) are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless written permission has been given by the Designated Safeguarding Lead, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

- Members of staff are not permitted to use their own personal phones or devices for contacting students or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Senior Designated Safeguarding Officer and/or Designated Safeguarding Lead

- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of students and will only use work-provided equipment for this purpose.
    - Directly with students, and will only use work-provided equipment during lessons/educational activities.

- If a member of staff breaches the College policy, action will be taken in line with the College behaviour and allegations policy

- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3. Students' Use of Personal Devices and Mobile Phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- The College expects pupil's personal devices and mobile phones to be switched off, kept out of sight during lessons and while moving between lessons)
- If a pupil needs to contact his/her parents or carers they will be allowed to use a College phone.
- Mobile phones or personal devices will not be used by students during lessons or formal College time unless as part of an approved and directed curriculum based activity with consent from a member of staff:

    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
    - If members of staff have an educational reason to allow students to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.

- Mobile phones and personal devices must not be taken into examinations:

    - Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.

- If a student breaches the College policy, the phone or device will be confiscated and will be held in a secure place:

    - College staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the College's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).

- Searches of mobile phone or personal devices will only be carried out in accordance with the College's policy. (See also www.gov.uk/government/publications/searching-screening-and-confiscation)
- Students' mobile phones or devices may be searched by a member of the management team, with the consent of the student or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes College policies.
- Mobile phones and devices that have been confiscated will be released to students or parents or carers at an appropriate and agreed time
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4. Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the College's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Safeguarding and Image use.
- The College will ensure appropriate signage and information is displayed/ provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Senior Designated Safeguarding Officer of any breaches of College policy.

9.5. Officially provided phones and mobile devices

- Members of staff will be issued with a work phone number and email address, where contact with students or parents/ carers is required.
- College mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- College mobile phones and devices will always be used in accordance with the Acceptable use policy and other relevant policies

10. RESPONDING TO E-SAFETY INCIDENTS AND CONCERNS

- All members of the College community will be made aware of the reporting procedure for e-safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content. (see RE16B for procedures)
- All members of the community must respect confidentiality and the need to follow the official College procedures for reporting concerns:

    - Students, parents and staff will be informed of the College's complaints procedure and staff will be made aware of the whistleblowing procedure.

- The College requires staff, parents, carers and students to work in partnership to resolve e-safety issues.
- After any investigations are completed, the College will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the College is unsure how to proceed with an incident or concern, the SDSO will seek advice from the local Safeguarding Team.

- Where there is suspicion that illegal activity has taken place, the College will contact the local Safeguarding Team or Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the College community (for example if other local Colleges are involved or the public may be at risk), the College will speak with local Police and/or the local Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1. Concerns about Students Welfare

- The SDSO will be informed of any e-safety incidents involving safeguarding or child protection concerns.
- The SDSO will record these issues in line with the College's child protection policy.
- The SDSO will ensure that e-safety concerns are escalated and reported to relevant agencies in line with the local multi-agency thresholds and procedures.
- The College will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2. Staff Misuse

- Any complaint about staff misuse will be referred to the Designated Safeguarding Lead, according to the Safeguarding policy on allegations.
- Any allegations regarding a member of staff's e- conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

11. USEFUL LINKS: NATIONAL LINKS AND RESOURCES

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/e-safety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional E-safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for Colleges: www.360safe.org.uk

12. Relevant Policies

RE 12 Acceptable use of Information and Communication Technologies
RE 15 Information Security
RE16b E-Policy Procedure
RE19 E-mail
RE21 Use of secure USB Memory sticks
GA23 Data Protection Policy