“Inspiring learning, developing character, building futures”

Student support policies and procedures

Online safety policy

Aim: The purpose of this online safety policy is to outline what measures the college takes to ensure that all members of the college community (including staff, students, volunteers, parents/carers, visitors, community users) can work in an e-safe environment and that any online safety issue is detected and dealt with in a timely and appropriate fashion.

Policy authorisation:	Management: Senior Leadership Team
Date of most recent update:	August 2023
Date of next policy review:	August 2024
Policy Author	Assistant Principal (Student Support)

Contents **Page Number**

1. Introduction 2

2. Scope of the policy 3

3. Roles and responsibilities 4

4. Education/training 6

5. Curriculum 7

6. Remote learning 8

7. Use of digital and video images 9

8. Filtering 9

9. Monitoring of internet use (students) 12

10. Reporting and responding to incidents 13

11. Review 14

1. Introduction

1.1. The rapid growth of the internet and of mobile electronic technologies has opened up a world of opportunities for students and staff. In their daily lives, students' use of the internet and digital technologies represent a seamless extension of the physical world. Many of today's students do not even notice they are using these technologies, with their emotional lives and development influenced by them. As online content, social networks and instant messaging converge with mobile technology to produce lives that are always 'on', any line that may have existed between being online and offline is disintegrating.

1.2. Through the internet and mobile technology it is possible for young people and adults to have access to almost unlimited information and communication worldwide. However, alongside the benefits there are also risks, especially if knowledge, understanding and appreciation of the risks is low. The main areas of risk for our college community can be summarised as follows:

Content
- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact
- Grooming (sexual and criminal exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct
- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Commerce
- Online gambling
- Iinappropriate advertising
- Phishing and or financial scams.
- If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group

1.3. Online safety is always about balancing opportunities with risks and we believe firmly in maximising opportunities and minimising risks. Blackpool Sixth believes that we must encourage students to develop as responsible online citizens. Such citizens will recognise their responsibility to keep themselves and their peers safe online. It is only through the development of a sense of online responsibility that we can ensure the safety and wellbeing of today's young people.

1.4. The college must be careful that "over blocking" does not lead to unreasonable restrictions that may impact teaching and learning.

2. Scope of the policy

a) 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 ICT systems, both in and out of college.

b) The Education and Inspections Act 2011 empowers college, 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 online bullying, or other online safety incidents covered by this policy, which may take place out of college, but is linked to membership of the college.

c) The college will deal with such incidents within this policy and associated positive behaviour and anti-bullying policies through the college disciplinary procedures and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of college.

3. Roles and responsibilities

3.1 Board of Directors:

a) Directors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.
b) Do all that is reasonably possible to limit students' exposure to risks from the college's IT system.
c) Ensure the college has appropriate filtering and monitoring systems in place and review their effectiveness.
d) Ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
e) Consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

3.2 Principal and the Senior Leadership Team

a) The Principal is responsible for ensuring the safety (including online safety) of members of the college community, though the day-to-day responsibility for leading online safety will be delegated to the Designated Safeguarding Lead (DSL).
b) The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).
c) The Senior Leadership Team will receive reports on online safety from the DSL as part of the safeguarding report.
d) The DSL will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

3.3 Designated Safeguarding Lead

a) Takes the lead responsibility for online safety (working together with the Network Manager and the Deputy Designated Safeguarding Leads).
b) Has an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
c) Ensures that all staff undergo online safety training at induction which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
d) Ensures that all staff have annual refresher/update training on online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
e) Ensures all staff understand the differences between filtering and monitoring and who is responsible for filtering and monitoring.
f) Ensures all staff know their role in terms of monitoring and reporting.
g) Ensures staff with specific roles in terms of online safety have appropriate training/knowledge that is relevant to their role.
h) Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety concern.
i) Review filtering and monitoring provision at least annually.
j) Conduct regular checks on the filtering and monitoring systems, at least once per term.
k) Liaises with the Local Authority and Police, as necessary.
l) Receives reports of online safety incidents and categorises appropriately to create a log of incidents to inform future developments
m) Monitors safe internet usage, using daily log file information, in collaboration with other Deputy Designated Safeguarding Leads

3.4 Network Manager:

The Network Manager is responsible for ensuring:

a) that the college's ICT infrastructure is secure and is not open to misuse or malicious attack.
b) that the college procures appropriate filtering and monitoring systems.
c) that the college meets the online safety technical requirements outlined in the Risk Management Policy and Acceptable Use of Computers Policy.
d) that users may only access the college's networks through a properly enforced password protection policy, in which passwords are regularly changed
e) the college's processes are applied and updated on a regular basis.

f) that he/she keeps up to date with online safety technical information in order to effectively carry out their role and to inform and update others as relevant.
g) that the use of the network/Virtual Learning Environments (VLEs) are regularly monitored in order that any misuse/attempted misuse can be reported to the Assistant Head of Student Services (Student Finance) for investigation.

The Network Manager will work with the DSL to:

a) review filtering and monitoring provision at least annually.
b) conduct regular checks on the filtering and monitoring systems, at least once per term.

3.5 Teaching and support staff

a) Have an up to date awareness of online safety matters and of the current online safety policy.
b) Have an understanding of the filtering and monitoring systems and who is responsible for filtering and monitoring.
c) Have understood and have signed the Acceptable Use of Computers Agreement.
d) Report any suspected misuse problem or concern about the welfare of a student via MyConcern or, if an immediate response is required, directly to the DSL or a member of the safeguarding team.
e) Communicate with students on a professional level and only carried out using official college systems.
f) Ensure online safety issues are embedded in all aspects of the curriculum and other activities.
g) Ensure students understand and follow the college online safety and acceptable use agreement.
h) Monitor ICT activity in lessons, extra curricular and extended college activities as far as is practically possible and report any concerns to the DSL or a member of the safeguarding team.
i) Use social media in a responsible and professional manner; please refer to the staff social media policy

3.6 The safeguarding team

a) Will be trained in online safety issues as listed in section 1.2
b) Will work alongside the DSL to respond appropriately to any online safety concerns

3.7 Students:

a) Are responsible for using the college ICT systems in accordance with the Acceptable Use of Computers Agreement, which they will be expected to 'accept' as part of their induction process.
b) Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
c) Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

d) Will be expected to know and understand college policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand college policies on the taking/use of images and on online bullying.
e) 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. Education/training

Whilst regulation and technical solutions are very important, their use must be balanced by educating members of college to take a responsible approach. Education in online safety is, therefore, an essential part of the college's online safety provision. Online safety education will be provided in the following ways:

4.1 Education – students

a) Planned online safety sessions will be provided as part of the pastoral curriculum– this will cover awareness of the safe use of ICT and new technologies both in college and outside college.
b) There are reported incidents of employers carrying out internet searches for information about potential and existing employees. The college will inform and educate students about these risks.
c) Key online safety messages should be reinforced through messages in the weekly notices provided by the Assistant Head of Student Services (Student Finance).
d) Students will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
e) Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

4.2 Education – staff

a) All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the college's online safety policy and Acceptable Use Policies.
b) Online safety training will form part of the safeguarding refresher training that all staff take part in annually. This training will include, amongst other things, an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
c) The DSL will receive regular updates through attendance at external training sessions and by reviewing guidance documents released by DfE, the local authority and others
d) The Assistant Head of Student Services (Student Finance) will provide any updates and reminders to staff through the staff weekly
e) This Online Safety Policy and its updates will be presented to and discussed by staff in Leadership Team and department meetings
f) The DSL will provide advice/guidance/training to individuals and teams as required
g) Staff should act as good role models in their use of ICT, the internet and mobile devices.

4.3 Education - Parents / Carers

a) Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. College will take every opportunity to help parents understand these issues through the website, social media, emails and letters.

5. Curriculum

Online safety should be a focus in all areas of the curriculum and staff should take any opportunities to embed online safety.

a) 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
b) Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
c) Students should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

6. Remote learning

Blackpool Sixth will ensure that any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements. However, it should be recognised that the college has limited control of student and staff personal devices and normal filtering and monitoring of network traffic cannot be applied while such devices are not connected to its network.

It is important that all staff who interact with students online continue to look out for signs that a student may be at risk. Any such concerns should be dealt with as per the Safeguarding and Child Protection Policy and where appropriate referrals should still be made to social care and, as required, the police.

Online risks are posed more by behaviours and values than the technology itself. Staff and students should ensure that they establish safe and responsible online behaviours when working remotely. To support this, the college will share safeguarding messages and online safety advice with all stakeholders via the college website, social media pages, student notices and pastoral mentors. This advice will include information on clear reporting routes so students and parents/carers can raise any concerns whilst online.

Communication with students both in the ‘real’ world and through web-based and telecommunication interactions should take place within explicit professional boundaries.

This means that staff should:

a) not request or respond to any personal information from students other than that which may be necessary for their professional role
b) ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'
c) not give their personal contact details to students or their parents/carers, for example, personal email address, home or mobile telephone numbers, details of web-based identities. If students locate these by any other means and attempt to contact or correspond with the staff member, the member of staff should not respond and must report the matter to their line manager
d) wherever possible, contact students and parents/carers using equipment provided by the college (e.g. college email, college phones, college mobiles or computer softphone which dials from the college number). It is strongly advised that staff don't use their personal mobile phone to contact students or parents/carers but where this is absolutely essential, staff **MUST** dial 141 (or use another secure method of ensuring your caller ID is not shown) before they dial the number so their personal contact details are not visible
e) use only the equipment and internet services provided/recommended by the college unless agreed with their line manager. The Google suite of apps should be used rather than other platforms such as WhatsApp or Zoom
f) follow the college's acceptable use of computers policy
g) ensure that their use of technologies (including social media) could not bring the college into disrepute

The college's Remote Learning Offer is available on the college website.

Staff should refer to the Protocols for using Google Meet with students document for guidance on how video calling can be used safely whilst students are learning remotely. There are three types of video call covered, each with slightly different protocols:

- "Live lesson" video calls with groups of students
- Video call meetings with students and their parents/carers/other adults
- 1:1 video call meetings between staff and students

It is important that staff have read and understood this document before conducting any real-time video calls with students.

7. Use of digital and video images

Staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

a) 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.
b) Staff are allowed to take digital/video images to support educational aims. These must be taken using a college device and follow good practice guidance concerning the sharing, distribution and publication of those images.

c) 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.
d) Images published on the college website, or any college social media, that include students will be selected carefully and will comply with GDPR guidance on the use of such images. This will include obtaining consent from any student who is clearly identifiable on any of the images used. It is the responsibility of the staff member taking the photo to ensure that this consent is obtained.
e) All students have the right to withdraw their consent at any time and can request the removal of any image published on the college website, or social media, that clearly identifies them. To do this students will need to contact the college Marketing Officer.

8. Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is, therefore, important that the college manages the associated risks and provides preventative measures which are relevant to the situation in this college.

a) The DSL takes lead responsibility for the filtering systems. The day-to-day responsibility for the management of the college's filtering procedures will be held by the Network Manager who will manage the college filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

b) The Network Manager will ensure any changes to the college filtering service are:

- reported to the DSL
- authorised by the DSL prior to changes being made
- recorded - including decisions on what is blocked or unblocked and why

c) All users have a responsibility to report immediately to the Network Manager or DSL any infringements of the college's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

d) Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

e) Students will be made aware of the importance of filtering systems through the pastoral curriculum. They will also be warned of the consequences of attempting to subvert the filtering system.

f) Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use of Computers Agreement
- induction training

- staff meetings, briefings, staff development

g) The following filtering rules will apply at all times:

Student filtering rules:

- Legal and liability issues
  - Child abuse
  - Drugs
  - Intolerance
  - Piracy and copyright infringement
  - Pornography
  - Self harm
  - Terrorism
  - Violence

- Adult themes
  - Abortion
  - Adult entertainers
  - Adult sites
  - Alcohol and tobacco
  - Criminal activity
  - Gambling
  - Gore
  - Naturism and nudism
  - Non-pornographic nudity
  - Restricted to adults
  - Sexuality sites

- Weapons
  - Hunting and sporting
  - Personal weapons

- Entertainment
  - Computer games
  - Jokes and humour
  - Online games

- File and image hosting
  - Image hosting:unmoderated image

- Finance
  - Payday loans

- Information and Reference
  - Plagiarism

- IT and technical

    - Peer-to-peer networking

- Lifestyle
    - Time-wasting

- Malware and hacking
    - Hacking
    - Malware and phishing
    - Web proxies

- Social media
    - Blogs
    - Dating sites
    - Discussion forums

- Web infrastructure
    - Parked domains

Staff filtering rules;

- Legal and liability issues
    - Intolerance
    - Piracy and copyright infringement
    - Pornography
    - Self harm
    - Terrorism
    - Violence

- Adult themes
    - Criminal activity
    - Gambling
    - Gore
    - Naturism and nudism
    - Non-Pornographic nudity
    - Restricted to adults
    - Sexuality sites

- Weapons
    - Hunting and sporting
    - Personal weapons

- File and image hosting
    - Image hosting: unmoderated image

9. Monitoring of internet use (students)

No filtering system can guarantee 100% protection against access to unsuitable sites. Members of the safeguarding team, therefore, monitor safe internet usage using daily logfile information produced by Smoothwall. The logfile identifies any inappropriate searches made by users during the previous 24 hours. The following categories are monitored:

- Abuse

- Bullying
- Radicalisation
- Suicide

Student monitoring procedures:

a) A member of the safeguarding team will conduct the daily monitoring of logfiles on a designated computer that has appropriate internet access and is not used by other members of the college.

b) Where there is a concern, a record is made of the URL, the name of the student, a summary of the nature of the concern and, where appropriate, screenshots are taken. Appropriate action will be taken that could include the following:

    - internal response - support, welfare, safeguarding or disciplinary
    - involvement of local authority
    - police involvement

c) If content involves the following material then monitoring and further investigation will be halted and referred to the police immediately:

    - child sexual abuse images
    - material which potentially breaches the Obscene Publications Act
    - radicalisation or links to extremism/terrorism
    - racist material
    - sexting
    - videoing assault using mobile phones
    - other criminal conduct, activity or materials

10. Reporting and responding to incidents

It is expected that all members of the college community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy may take place through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

a) Students should report an incident to their Progress Mentor or any other member of staff.

b) Members of staff must report any incidents concerning online safety via MyConcern or, if an immediate response is required, directly to the DSL or a member of the safeguarding team.

c) All reported online safety incidents will be taken very seriously and will be investigated by a member of the safeguarding team. The college will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

d) If any apparent or actual misuse appears to involve illegal activity then the incident must be reported to the DSL or a member of the safeguarding team. Steps will be taken to ensure that evidence is preserved and the police will be informed. Possible illegal activity includes:

- child sexual abuse images
- material which potentially breaches the Obscene Publications Act
- radicalisation or links to extremism/terrorism
- racist material
- sexting
- videoing assault using mobile phones
- other criminal conduct, activity or materials

e) 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. Incidents of misuse will be dealt with through the positive behaviour policy and disciplinary procedures. Possible misuse includes:

- Inappropriate use of any internet or digital technologies
- Unauthorised use of non-educational sites during lessons/unauthorised downloading or uploading of files
- Using proxy sites or other means to subvert the college's filtering system
- Attempting to access or accessing the college network, using another person's account or allowing others to access college network by sharing username and passwords
- Corrupting or destroying the data of other users
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Actions which could bring the college into disrepute or breach the core values of the college
- Actions which could compromise the professional reputation of a member of the college

f) Following any investigation, the college will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place and external agencies may be involved depending on the seriousness of the incident.

g) Sanctions may include:

- removal of internet or computer access for a period
- informing parents or carers
- supervised study
- external agencies such as social networking or email member sites may be contacted and informed.
- college disciplinary procedures including formal warnings, suspension and exclusion, where applicable
- referral to the Police or local authorities

h) Any staff misuse that suggests a crime has been committed, a student has been harmed or that a member of staff is unsuitable to work with children will be reported to the LADO in accordance with Blackpool Safeguarding Children Board policies.

11. Review

a) The DSL will monitor the implementation and impact of this online safety policy using:

- logs of reported incidents
- focus groups
- surveys/questionnaires of students, parents/carers and staff
- learning from case reviews

b) The Senior Leadership Team and Board of Directors will receive a report on the implementation of the online safety policy each year as part of the safeguarding report. This report will include details of online safety incidents and actions undertaken.

c) The content and operation of this policy will be reviewed annually by the DSL and Network Manager. The policy may be reviewed more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.