DN COLLEGES GROUP

E-Safety Policy

Effective from: September 2019

Version Number: I

1. Purpose

1.1 DN Colleges Group (DNCG) recognises both the benefits and opportunities that new technologies afford teaching, learning and assessment. That said, the global nature of the internet and the variety of technologies now available, mean that we need to implement safeguards that enable staff, students and apprentices to identify and manage risks associated with their use. We believe that this can be achieved through a combination of security measures, training, guidance and support as well as the implementation of associated policies.

We acknowledge how new technologies have increasingly become embedded and sometimes integral to the lives of our students/apprentices both within college and in their lives outside of college. In addition, we understand and encourage the use of technology to engage students/apprentices, enhance teaching, learning and assessment and help improve achievement. Furthermore, we recognise the importance of using technology to develop Digital Literacy skills and better prepare students/apprentices for employability in a digital society.

However, we acknowledge the potential risks associated with the use of these technologies including awareness of Government policies relating to Safeguarding & PREVENT so to this end our policy sets out our approach to managing these risks. We recognise our safeguarding duties and aim to ensure all staff, students and apprentices are supported effectively to ensure they provide a safe learning environment for all and empower them to manage their own online safety.

E-safety has a significant overlap with other policies and procedures, particularly those related to

- Safeguarding
- ICT Systems Acceptable Use
- Staff/Student Code of Conduct
- Data Protection/General Data Protection Regulations (GDPR)
- Marketing & Communications
- Inclusion, Equality & Diversity
- Social Media

2 Scope

2.1 This policy applies to all members of the college community, not limited to staff, students, apprentices, governors, volunteers, parents/carer and visitors, who have access to and are users of college ICT systems and applies both in and out of physical college spaces. The DNCG centres will ensure that all users of technologies adhere to the expected standard of behaviour as set out in the Code of Conduct.

2.2 An E-safety incident is considered to have occurred when a Student, Apprentice, Staff Member or Governor instigates, or is the victim of, an activity which utilises Information and Communications Technologies (ICT) to endanger the personal safety, mental wellbeing or financial well-being of another individual.

Activities which will be considered E-safety incidents, include but are not limited to, the use of ICT to:

Access, view, copy or download illegal content, or materials, including but not limited to:

- child pornography
- materials inciting racial hatred or violence
- materials that are deemed to be in connection with radicalisation or will place students/apprentices at risk of radicalisation
- Access, view, copy or download inappropriate content, or materials, as defined by DNCG's Acceptable Use of IT policy
- Bully or harass an individual or group (cyber bullying)
- Commit fraud
- Any other incident where it can be reasonably considered that the personal safety, mental wellbeing or financial health of an individual has been endangered by the use of ICT
- Undertake any activities which would be in violation of the following policies:
    - ○ Safeguarding
    - ○ ICT Systems Acceptable Use
    - ○ Staff/Student Code of Conduct
    - ○ Data Protection
    - ○ Marketing & Communications

    - ○ Inclusion, Equality & Diversity Policy
    - ○ Social Media

In this context, ICT includes but is not limited to:

a) College owned equipment

- Desktop PCs
- Servers
- Laptop/tablet devices
- Telephones, both fixed and mobile
- Digital video camera or camcorders
- Digital audio recording devices
- Reproduction devices (scanners, printers, etc.)
- Any and all software and IT services provided by the DN Colleges Group

b) Privately owned ICT equipment (including personal mobile phones), when:

- Connected to any College owned network
- Utilised to access College software and services
- Made use of on campus, or in the pursuit of College business

3 Responsibilities

3.1 **It is the responsibility of every staff member to give full and active support for the policy by ensuring:**

College Staff

- The policy is accessible, known, understood and implemented

- All actual and suspected serious E-safety incidents are reported to the Safeguarding team using CPOMS.
- Parents/guardians, providers, sponsors, employers and other stakeholders have a responsibility to report any E-safety concerns they may have to the College.
- To have an up to date awareness of online safety matters and the current college online safety policy and practices.
- Online Safety activities are embedded in all aspects of the curriculum and other appropriate activities.
- To use college online systems and tools in accordance with the college IT Guidelines and ICT Acceptable Use policy.

All Students/Apprentices, both within Further and Higher education, have a responsibility to:

Students/Apprentices

- Report any E-safety concerns that they may have to a member of staff, (teaching, support or Business Services)
- Not engage at any time in any form of behaviour, which would result in the occurrence of an E-safety incident
- Are responsible for using college digital technology and systems in accordance with Acceptable Usage policies.
- Have a good knowledge of online safe practices including but not limited to: the importance of reporting abuse, the need to avoid plagiarism and uphold copyright regulations

Implementing online safety is the responsibility of all and closely mirrors safeguarding responsibilities. Specific roles in relation to online safety are defined as such:

Governors

- Governors are responsible for the approval and reviewing the effectiveness of the E-safety Policy.

E-safety Working Group

- Responds to changes and adapt the policy where required.
- Provides training and advice for staff using online technologies as part of teaching, learning and assessment.
- Liaises with college technical staff.
- Review and monitoring of the E-safety Policy.
- Monitoring improvement actions identified through bi-annual reviews IT/Network Team.
- Supports Safeguarding team with E-safety concerns and resolutions, including CPOMS, Visigo and internet monitoring.

IT Support Team

- To ensure DNCG systems and infrastructure are secure and not open to misuse and malicious attack.
- That the use of the network is regularly monitored as far as possible to prevent misuse.
- Provide reporting of internet logs to E-safety group. To ensure websites and student access is blocked or restricted as required.

Safeguarding Team

- Is trained in online safety issues and be aware of the potential for serious safeguarding issues that may arise from: Sharing of personal data, accessing illegal/harmful materials, inappropriate online contact with others, incidents of grooming and cyber bullying.
- Routinely check internet logs and Visigo for internet misuse, to act upon these.
- To ensure E-safety concerns raised via members of staff / CPOMS are investigated resolved and actioned, that an audit trail and action trial has been logged on CPOMS.
- Work closely with E-safety working group to ensure information is shared and any E-safety concerns are resolved

Prevent, Equality & Diversity Leader

- Trained in online safety issues and working collaboratively with external partners with awareness of the potential for serious safeguarding issues that may arise from: violent extremism, Islamist ideology, far right/Neo Nazi/White supremacist ideology.

Senior Leaders

- To ensure there is a system in place to allow for the monitoring and ongoing support of online safety relating to members of the college community.

4 Definitions and/or Relevant Legislation

4.1 The legal framework for the role of the Group and the governing body is as follows:

Computer Misuse Act 1990

Makes provision for securing computer material against unauthorised access or modification; and for connected purposes.

Data Protection Act 1988

Makes provision for the regulation of the processing of information relating to individuals, including obtaining, holding, use or disclosure of such information.

Malicious Communication Act 1998

Makes provision for the punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety.

Working Together to Safeguard Children and Young People (2018)

Provides statutory guidance on the roles and responsibilities of agencies working together to safeguard children/young people. In addition, it sets out the framework for local safeguarding arrangements and details the allegation management process.

Mental Capacity Act 2005

Provides a way in which people who may need help to make decisions can get that help from someone who can be trusted to act in their best interests. Mental Capacity under the Act means being able to make your own decisions. The Mental Capacity Act and its Code of Conduct contains a set of rules, procedures and guidance.

5 The Policy

5.1 Safeguarding our students/apprentices is at the centre of our E-safety policy and college values. The DN Colleges Group also believes positive use of technology including the use of online resources, communications and social media can greatly enhance the student's/apprentice’s experience. Thus we require the correct guidance and support to ensure staff, students and apprentices are empowered to use modern technologies in a way that engages and motivates them whilst promoting its safe use.

We consider staff and student Content, Contact and Conduct with the use of online technologies. The college champions E-safety advice directly from CEOP and Internet Matters, E-safety Posters are displayed. Staff E-safety advice should also be displayed in staff rooms. In addition, E-safety training is an integral part of the college tutorial scheme, as well as planned events throughout the academic year to raise awareness of E-safety online generally.

Additional training and guidance is available for staff. Staff will be expected to complete mandatory online training in E-Safety with this also formally included as part of the college induction process. Staff will be expected to keep up to date with E-Safety concerns and issues via online and face to face training. E-safety is also part of the new staff induction process both online and via face to face on the new staff induction process and mandatory child protection training.

Social Media

We recognise that new technologies provide additional opportunities for staff, students and apprentices to participate in interactive online discussions and share information on particular topics, by using a wide variety of social media, such as Facebook, Twitter, blogs and more. We also recognise the value of Social Media tools for supporting Employability and engaging with the extended college community as well as interacting with employers, parents/carers and prospective students/apprentices.

5.2

The college requires that all users using social media adhere to the standard of behaviour as set out in the **Social Media Policy**, as well as but not limited to

- Safeguarding
- ICT Systems Acceptable Use

- Staff/Student Code of Conduct
- Data Protection/GDPR
- Marketing & Communications
- Inclusion, Equality & Diversity

Personal and Mobile Devices

Personal and mobile devices have become significantly embedded in the everyday lives of many staff, students and apprentices. Having access to digital technology has changed the way in which learning is delivered. The college embraces opportunities to maximise the use of these technologies, where appropriate, and recognises this provides opportunities to deepen learning and enhance the digital literacy skills of staff and students/apprentices. Staff, students and apprentices must understand the primary purpose of these devices at college is educational and staff should carefully consider the outcome and impact before using such technology within teaching. The key to successful use in teaching, learning and assessment lies with good classroom management and educating students/apprentices on the correct use of technology. The DN Colleges Group also recognises that not all students/apprentices have access to personal devices and staff should
5.3 consider this before using such technologies.

- All college devices are controlled through the use of Mobile Device Management software.
- Staff/Students will benefit from free Wifi access for mobile devices but filtering will be applied to the internet connection and attempts to bypass this are not permitted.
- Personal devices are brought into the college entirely at the risk of the owner and the decision to bring the device in lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in college.
- The college recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the college. Pass-codes or PINs should be set on personal devices to aid security.
- Devices may not be used in tests or exams.
- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements.
- Students, apprentices and staff are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network.
- Staff, student and apprentice owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances.

Monitoring, Review and Dissemination

The College reserves the right to monitor usage of its computing facilities, in order to ensure their proper use according to IT Guidelines, Acceptable Use and E-Safety policies. Monitoring is permanently in place and may also be undertaken randomly or at fixed periods dependent upon the computing facility. Please see the ICT Systems Acceptable Use Policy in the first instance.

Security

College networks are safe and secure, with appropriate and up-to-date security measures and software in place. The college IT team are 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.

- There will be regular reviews and audits of the safety and security of college academy technical systems
- 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 by the college ICT support team. Users are responsible for the security of their username and password and will be required to change their password every 90 days.
- Illegal content (e.g. child sexual abuse images etc) is filtered by the broadband or requirements
- All safety incidents can be reported anonymously via the college website using the text message or forms available
- Appropriate security measures are in to protect the servers, firewalls, routers, wireless systems, work stations, an up to date record of users and their usernames.

Risk Assessment

When making use of new technologies and online platforms, staff are to assess the potential risks that they and their students could be exposed to:

Behaviour

- It is unacceptable to download or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory, related to violent extremism or terrorism or which is intended to annoy, harass or intimidate another person. This also applies to the use of social media accessed from College systems.

- All users of technology adhere to the standards of behaviour set out in the ICT Systems Acceptable Use Policy.

- All users of IT adhere to College guidelines when using email, mobile phones, social networking sites, games consoles, chat rooms, video conferencing and web cameras etc.

- Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) are dealt with seriously, in line with staff and student disciplinary procedures.

- Staff must take responsibility for moderating any content posted online.

- Staff should be aware of cyber bullying, grooming law and child protection issues and forward any concerns to the safeguarding team.

- Staff should keep personal and professional lives separate online.

- Staff should not have students/apprentices as *friends* on social media sites that share personal information, as clearly defined within the Social Media Policy.

- Staff should be wary of divulging personal details online and are advised to look into privacy settings on sites to control what information is publicly accessible.

- Staff should recognise that they are legally liable for anything they post online.

- Staff are expected to adhere to the DN Colleges Group Inclusion, Equality and Diversity Policy at all times, and not post derogatory, offensive or prejudiced comments online.

- Staff should not bully or abuse colleagues/students online.

- Staff entering into a debate or discussion with a student/apprentice online should ensure that their comments reflect a professional approach.

- Staff should not post any comments online that may bring DN Colleges Group into disrepute or that may damage the Group's reputation.

- Staff wishing to debate and comment on professional issues using personal sites, should be aware that this may be seen as a reflection of college views, even with a disclaimer, and should consider their postings carefully.

- Staff should not use their college email address to join sites for personal reasons or make their college email address their primary contact method.

- Staff should be aware that any reports of them undertaking any inappropriate online activity that links them to DN Colleges Group, will be investigated and may result in disciplinary action.

Use of Images and Video

- The use of images or photographs is encouraged in teaching and learning, providing there is no breach of copyright or rights of another person.

- Staff, students and apprentices are trained in the risks of downloading, posting and sharing images, and particularly the risks involved in posting personal images onto social networking sites for example.

- College staff provide information to students/apprentices on the appropriate use of images, and on how to keep their personal information safe.

- Advice and approval from a senior manager is sought in specified circumstances or if there is any doubt about the publication of any materials.

Personal Information

- Processing of personal information is done in compliance with the Data Protection Act 1998.
- Personal information is kept safe and secure and is not passed on to anyone else without the express permission of the individual.
- No personal information is posted to the DN Colleges Group websites/intranets without the express permission of the individual.
- Staff keep students'/apprentices' personal information safe and secure at all times.
- When using an online platform, all personal information is password protected.
- No personal information of individuals is take off-site unless the member of staff has the permission of their manager and the data is secured.
- College mobile devices that store sensitive information are encrypted and password protected.
- Personal data no longer required, is securely deleted.

Education and Training

- Any new or temporary users receive training on the college IT systems, they are also asked to read, agree and sign an ICT Systems Acceptable Use Policy.

- Inductions and the tutorial programme contains sessions on E-safety.

- Students/apprentices are guided in E-Safety across the curriculum and opportunities are taken to reinforce E-Safety messages.

- Students know what to do and who to talk to where they have concerns about inappropriate content, either where the material is directed to them, or where it is discovered as part of a random search.

- In classes, students/apprentices are encouraged to question the validity and reliability of materials researched, viewed or downloaded. They are encouraged to respect the copyright of other parties and to cite references properly.

- Staff, students and apprentices are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively.

- It is essential that all staff receive mandatory training and understand their responsibilities as outlined in this policy

- A planned programme of formal online safety training will be made available to existing and new staff. This will be regularly updated and reinforced.

- The college will seek to inform and update parents and carers through: parents evenings, curriculum activities and college open events, social Media communications, newsletters and Website updates and high profile events such as Safer Internet Day

Incidents and Response

- A clear and effective incident reporting procedure is maintained and communicated to students and staff. (See appendix). All reporting regarding E-safety concerns are to be submitted via CPOMS. Issues regarding staff should be reported directly to Safeguarding.

- The DN Colleges Group uses internet filtering and logging via internal and external systems. These systems will alert the relevant individuals of the concern or incident, such as an attempt to access and illegal site. Individuals will log filtering / alerts via CPOMS alongside actions that resolved the incident. (see appendix)

- Reports of E-safety incidents are acted upon immediately to prevent, as far as possible, any harm or further harm occurring.

- Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies (e.g. the police), review of internal procedures and safeguards, tutor support for affected students/apprentices.

6 Relevant Policies and Procedures

6.1

- Copyright Policy
- ICT Systems Acceptable Use Policy
- Data Protection Policy/GDPR
- Inclusions, Equality and Diversity Policy
- Safeguarding Policy
- Social Media Policy
- Marketing and Communications.

7 Who to contact with Queries

7.1 Filter all queries through the service desk to be escalated as appropriate.

- Digital Teaching and Learning Manager, phil.whitehead@northlindsey.co.uk
- Head of Marketing, emma.turner@northlindsey.ac.uk
- Head of HR & OD, scott.wilson@northlindsey.ac.uk
- Director of Digital Technologies, steve.patterson@dncolleges.co.uk
- Head of Academic Services, sarah.crossland@don.ac.uk
- Associate Director, Safeguarding & Prevent,
- Deputy Principal, kit.sargent@northlindsey.ac.uk

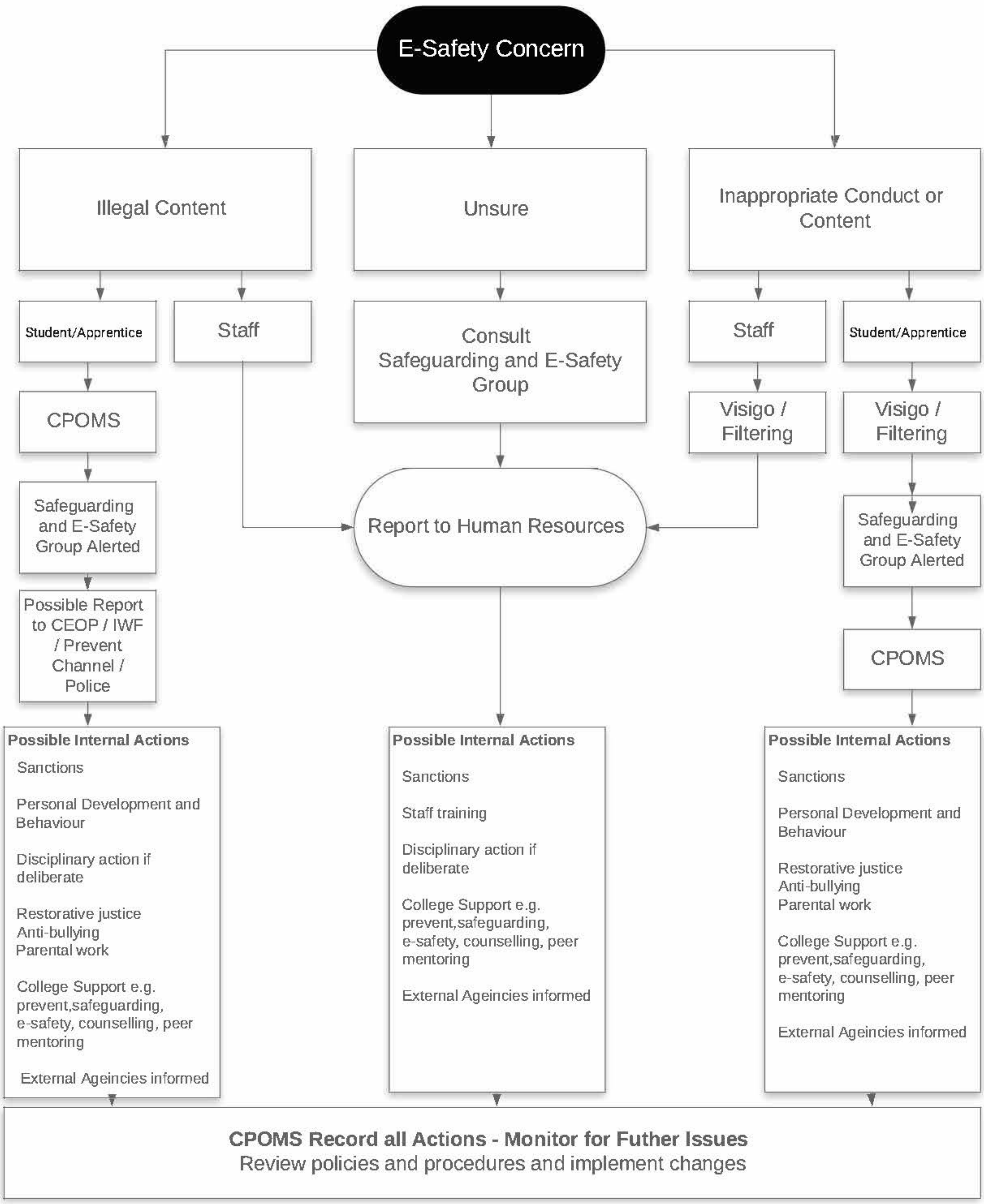
8 Communication

8.1 The policy will be communicated via the normal online and offline channels, for example the Group Intranet, Email, Face to Face sessions and an online training Module.

9 Authorisation

Policy Holder:	Deputy Principal
Committee Group:	Safeguarding Group
Authorising Group:	Senior Leadership Team
Initial Authorisation:	4 October 2019
Review Date:	November 2021

E-Safety
Reporting and


E-Safety Concern
Illegal Content
Unsure
Inappropriate Conduct or Content
Student/Apprentice
Staff
Consult Safeguarding and E-Safety Group
Staff
Student/Apprentice
CPOMS
Visigo / Filtering
Visigo / Filtering
Safeguarding and E-Safety Group Alerted
Report to Human Resources
Safeguarding and E-Safety Group Alerted
Possible Report to CEOP / IWF / Prevent Channel / Police
CPOMS
Possible Internal Actions
Sanctions
Personal Development and Behaviour
Disciplinary action if deliberate
Restorative justice
Anti-bullying
Parental work
College Support e.g. prevent,safeguarding, e-safety, counselling, peer mentoring
External Ageincies informed
Possible Internal Actions
Sanctions
Staff training
Disciplinary action if deliberate
College Support e.g. prevent,safeguarding, e-safety, counselling, peer mentoring
External Ageincies informed
Possible Intemal Actions
Sanctions
Personal Development and Behaviour
Restorative justice
Anti-bullying
Parental work
College Support e.g. prevent,safeguarding, e-safety, counselling, peer mentoring
External Ageincies informed
CPOMS Record all Actions - Monitor for Futher Issues
Review policies and procedures and implement changes