ADVENIAT REGNUM TUUM

Archbishop Beck Catholic Sports College

On-Line Safety Policy

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the college community at Archbishop Beck Catholic Sports College with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist college staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole college community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other college policies].
- Ensure that all members of the college community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

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 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 well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Archbishop Beck community (including ALL staff, students/students, volunteers, parents/carers, visitors, community users) who have access to and are users of college IT systems, both in and out of Archbishop Beck.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance. • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole college safeguarding. • To take overall responsibility for online safety provision. • To take overall responsibility for data management and information security ensuring college's provision follows best practice in information handling and is compliant with the eight principles of the Data Protection Act 1998. • To ensure the college uses appropriate IT systems and services including, a filtered Internet Service. • To be responsible for ensuring that ALL staff receive suitable training to carry out their safeguarding and online safety roles. • To be aware of procedures to be followed in the event of a serious online safety incident. • Ensure suitable 'risk assessments' are undertaken so the curriculum meets the needs of students, including the risk of children being radicalised. • To receive regular monitoring reports from the Online Safety Lead. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager. • To ensure Governors are regularly updated on the nature and effectiveness of the college's arrangements for online safety. • To ensure college that the college website includes relevant information and is compliant with the statutory requirements.
Online Safety Lead/Designated Safeguarding Lead (this may be the same person)	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the college's online safety policy/documents. • Promote an awareness and commitment to online safety throughout the college community.

Role	Key Responsibilities
	• Ensure that online safety education is embedded within the curriculum. • Liaise with college technical staff where appropriate. • To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and appropriate filtering/monitoring issues and change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident. • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for ALL staff. • Oversee any student surveys/student feedback on online safety issues. • Liaise with the Local Authority and relevant agencies. • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Safeguarding governor (including online safety)	• To ensure that the college has in place policies and practices to keep the children and ALL staff safe online. • To approve the Online Safety Policy and review the effectiveness of the policy. • To support the college in encouraging parents/carers and the wider community to become engaged in online safety activities. • The role of the Online Safety Governor will include: regular review with the Online Safety Lead
Computing Curriculum Lead	• To oversee the delivery of the online safety elements of the Computing Curriculum.
Network Manager/IT technician	• To report all online safety related issues that come to their attention, to the Online Safety Lead. • To manage the college's computer systems, ensuring - college password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus/malware/ransomware protection up to date). - access controls/encryption exist to protect personal and sensitive information held on college-owned devices. - the college's policy on appropriate web filtering and monitoring is applied and updated on a regular basis. • To keep up to date with the colleges online safety policy and technical information in order to effectively carry out their

Role	Key Responsibilities
	online safety role and to inform and update others as required. • To ensure college technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Online Safety Lead/DSL/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place, • To keep up-to-date documentation of the college's online security and technical procedures.
Data and Information Managers	• To ensure that the data they manage is accurate and up-to-date. • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The college must be registered with Information Commissioner.
Teachers	• To embed online safety in the curriculum. • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended college activities if relevant). • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the college staff Acceptable Use Policy, and understand any updates - annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problems to the Online Safety Lead. • To maintain an awareness of current online safety issues and guidance e.g. through relevant CPD. • To always model safe, responsible, respectful and professional behaviours in their own use of technology. **Exit strategy** • At the end of the period of employment returning any equipment or devices loaned by the college. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Role	Key Responsibilities
Students	• Read, understand, sign and adhere to the Student /Student Acceptable Use Agreement, annually. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To understand the importance of adopting safe, responsible and respectful behaviours and 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. • To contribute to any 'student voice'/surveys that gathers information of their online experiences.
Parents/carers	• To read, understand and promote the college's Student Acceptable Use Agreement with their child/children. • To consult with the college if they have any concerns about their children's use of technology. • To support the college in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet, including social media and the college's use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology or the Internet within college. • To support the college in promoting online safety. • To model safe, responsible, respectful and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/students/community in the following ways:

- Policy to be posted on the college website.
- Policy to be part of college induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable Use Agreements discussed with staff and students at the start of each year. Acceptable Use Agreements to be issued to whole college community, on entry to the college.

Handling Incidents:

- The college will take all reasonable precautions to ensure online safety.
- Staff and students are given information about infringements in use and possible sanctions.
- Online Safety Lead to act as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Lead that day.

- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

The Online Safety Policy is referenced within other college policies (e.g. Safeguarding and Child Protection Policy, Anti-Bullying Policy).

- The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the college.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the college Online Safety Policy will be disseminated to all members of staff and students.

2. Education and Curriculum

Student online safety curriculum

This college:

- has a clear, progressive online safety education programme as part of the ICT / Computing Curriculum and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the Student Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe, responsible, respectful and professional behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure students only use college-approved systems and publish within appropriately secure/age-appropriate environments.

Staff and governor training

This college:

- makes regular training available to staff on online safety issues and the college's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the college's Acceptable Use Policies/Agreements.

Parent awareness and training

This college:

- publishes appropriate information and guidance on on-line safety on the college website and signposts where additional information is available.

3. Expected Conduct and Incident management

Expected conduct

In this college, all users:

- are responsible for using the college IT and communication systems in accordance with the relevant Acceptable Use Policies/Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting safe, responsible and respectful online safety practice when using digital technologies in and out of college;
- know and understand college policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access;
- know to take professional, reasonable precautions when working with students, previewing websites before use; using age-appropriate (student friendly) search engines where more open Internet searching is required with younger students;

Parents/Carers

- should provide consent for students to use the Internet, as well as other technologies, as part of the Online Safety Acceptable Use Agreement form;
- should know and understand what the college's 'rules of appropriate use for the whole college community' are and what sanctions result from misuse.

Incident Management

In this college:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;

- all members of the college are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the college's escalation processes;
- support is actively sought from other agencies as needed (i.e. College Improvement Liverpool, UK Safer Internet Centre Helpline (0844 3814772/helpline@saferinternet.org.uk), CEOP, Prevent Officer, Merseyside Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the college;
- parents/carers are specifically informed of any online safety incidents involving young people for whom they are responsible;

- the Police will be contacted if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Merseyside Police, Internet Watch Foundation and inform the Local Authority.

4. Managing IT and Communication System

Internet access, security (virus protection) and appropriate filtering and monitoring

This college:

- informs all users that Internet/email use is monitored;
- has filtered, secure broadband connectivity provided by British Telecom – CAW Broadband;
- uses Lightspeed Rocket Appliance which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- uses user-level filtering where relevant;
- ensures network health through use of ESET anti-virus software;

Network management (user access, backup)

This college

- Uses individual, audited log-ins for all users – Windows domain logons;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Ensures the Systems Administrator/Network Manager is up-to-date with their technical knowledge;
- Has daily back-up of college data (admin and curriculum);

To ensure the network is used safely, this college:

- Ensures staff read and sign that they have understood the college's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the college's network.
- All students have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the college and/or connected to the network has up to date virus/malware/ransomware protection;
- Makes clear that staff are responsible for ensuring that any computer/laptop/mobile device loaned to them by the college, is used only to support their professional responsibilities.

- Makes clear that staff accessing Local Authority systems do so in accordance with any corporate Liverpool City Council policies;
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the college's network resources from remote locations by staff is audited and restricted and access is only through college approved systems;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited, restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off-site back up of data;
- This college uses secure data transfer. (Collect, S2S and Common Transfer Files)
- Our wireless network has been secured.
- All IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This college makes it clear that staff and students must always keep their passwords private, must not share with others. If a password is compromised the college should be notified immediately.
- All staff have their own unique username and private passwords to access college systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.

E-mail

This college

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- We use a number of technologies to help protect users and systems in the college, including desktop anti-virus products, plus direct email filtering for viruses.

Students:

- Students are taught about the online safety and 'netiquette' of using e-mail both in college and at home.

Staff:

- Staff will use the college e-mail systems for professional purposes.

College website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The college web site complies with statutory DFE requirements;
- Photographs published on the web do not have full names attached. We do not use students' names when saving images in the file names or in the tags when publishing to the college website;

Cloud Environments

- Uploading of information on the college's online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the college's online environment will only be accessible by members of the college community;
- In college, students are only able to upload and publish within college approved 'Cloud' systems.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for students use on a personal basis or to open up their own spaces to their students, but to use the colleges' preferred system for such communications.

College staff will ensure that in private use:

- No reference should be made in social media to students/students, parents/carers or college staff.
- Never post images or videos of students/students.
- College staff should not be online friends with any students/students or parents/carers of students/students.
- If they receive a friend request from a student/student or parent/carer they should decline the invite and inform their Line Manager.
- They do not engage in online discussion on personal matters relating to members of the college community;
- Personal opinions should not be attributed to the college and personal opinions must not compromise the professional role of the staff member, nor bring the college into disrepute;
- Security and privacy settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Students:

- Are taught about social networking, safe, responsible, respectful and acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.
- Are encouraged to model safe, responsible and respectful use of social media for their children to emulate.
- As a college we believe that parents should be discouraged from using social media to criticise teaching staff and to make comments about our college and the community it serves. If you feel that you have any issues regarding your child's collegeing, please make an appointment to come and talk to us. We are always happy to listen.

CCTV

- We have CCTV in the college as part of our site surveillance for staff and student safety.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this college:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key college information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised to.
- All staff are DBS checked and records are held in a single central record.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer.
- All servers are in secure, lockable locations and managed by DBS-checked staff.
- Details of all college-owned hardware will be recorded in a hardware inventory, including hardware on loan to named staff members.
- Details of all college-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into college are entirely at the staff member, students & parents or visitors own risk. The College accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into college.
- Personal mobile devices will not be used during lessons or formal college time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- Student personal mobile devices, which are brought into college, must be turned off (not placed on silent) and stored out of sight on arrival at college. They must remain turned off and out of sight until the end of the day.
- Personal mobile devices will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The College reserves the right to search the content of any mobile devices on the college premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. (see separate guidelines on dealing with a device where there is suspicion of illegal content).
- If a student needs to contact his or her parents or carers, they will be allowed to use a college phone. Parents are advised not to contact their child via their mobile phone during the college day, but to contact the college office.

Storage, Synchronizing and Access

The device is accessed with a college owned account

- The device has a college created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a college owned mobile device, staff must be aware that college use will be synched to their personal cloud, and personal use may become visible in college and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students' use of personal devices

- If a student breaches the college policy, then the device will be confiscated and will be held in a secure place.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff using mobile phones or hand held devices holding images or files taken in college must be downloaded from the device and deleted in college.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a college phone where contact with students, parents or carers is required, for instance for off-site activities.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- In an emergency where a staff member doesn't have access to a college-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the college policy then disciplinary action may be taken.

Digital images and video

In this college:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the college agreement form or when their daughter/son joins the college;
- Staff sign the college's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students;
- If specific student photos (not group photos) are used on the college web site, in the prospectus or in other high profile publications the college will obtain individual parental or student permission for its long term, high profile use.
- The college blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Students are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images

that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Dealing with a device where there is suspicion of illegal content

Staff have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the college rules.

- Searching with consent – Staff may search with the student's consent for any item.
- Searching without consent – Staff may only search without the student's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the college rules as an item which is banned and may be searched for.

IN CARRYING OUT THE SEARCH

The authorised member of staff must have reasonable grounds for suspecting that a student is in possession of a prohibited item i.e. an item banned by the college rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment.

The member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties eg a visiting parent or contractor, only to devices in the possession of student's).

The member of staff should take care that, where possible, searches not take place in public places eg an occupied classroom, which might be considered as exploiting the student being searched.

The member of staff carrying out the search must be the same gender as the student being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student being searched.

There is a limited exception to this rule: Staff can carry out a search of a student of the opposite gender including without a witness present, **but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

EXTENT OF THE SEARCH

The person conducting the search may not require the student to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the student has or appears to have control – this includes desks, lockers and bags.

A student's possessions can only be searched in the presence of the student and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (eg a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the college rules regardless of whether the rules say an item can be searched for.

Further information relating to searching students can be found in this Department of Education document (published Feb 14) www.gov.uk/government/publications/searching-screening-and-confiscation. Use of reasonable force guidelines www.gov.uk/government/publications/use of reasonable force July 2013.

ELECTRONIC DEVICES

A member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the college rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the college open to legal challenge.

Archbishop Beck Catholic Sports College

On-Line Safety Log

This incident log will be monitored termly by the Headteacher and ICT Steering Group.

Date & Time	Name of Student or Staff member	Room and computer / device number	Details of incident (including evidence	Actions	Name and role of person completing this entry

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	

Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of Second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for websites)

Website(s) address / device **Reason for concern**

Conclusion **Action proposed or taken**

E-safety Log

Name of Student Involved:	**Name of Staff Identifying Issue:**
Date of Reporting:	**Person Reported to:**
Nature of Incident/Concern:	**Action Taken:**

<table>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>Area Where Incident Occurred:</b></td><td colspan="2"><b>At What Point Concern was Identified:</b></td></tr>
<tr><td colspan="3"><b>Further Recommendations/Actions:</b></td><td><b>By Whom:</b></td></tr>
<tr><td colspan="3"><b>Sanctions Applied(where appropriate):</b></td><td><b>By Whom:</b></td></tr>
<tr><td><b>Person Completing this Entry:</b>
<b>(Please print)</b></td><td colspan="2"><b>Signature:</b></td><td><b>Date:</b></td></tr>
</table>

SWFgL Esafety College Template Policies

360safe

The Esafety Self Review Tool

Online Safety Incident

Unsuitable materials

Illegal materials or activities found or suspected

Report to the person responsible for Online Safety

Illegal Activity or Content (No immediate risk)

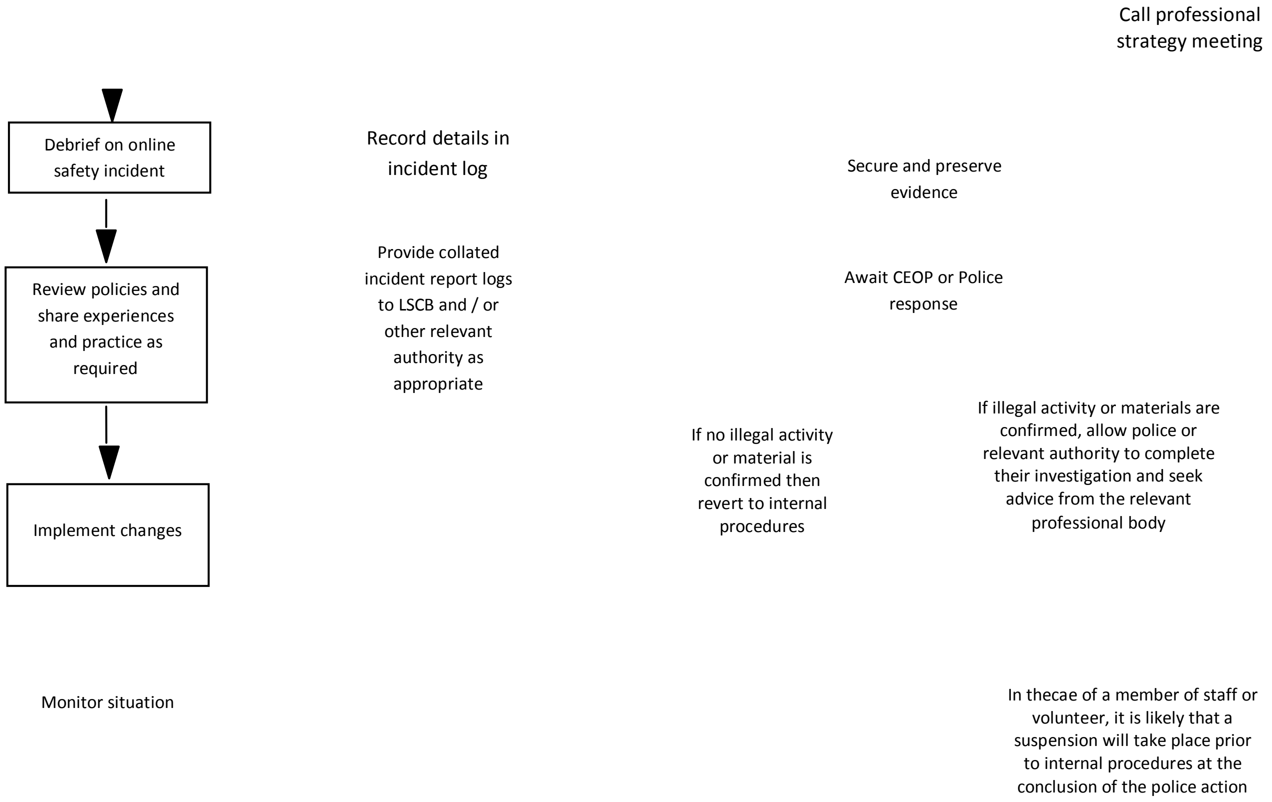
Illegal Activity or Content (Child at Immediate Risk)

Staff / Volunteer or other adult

If staff / volunteer or child / young person, review the incident and decide upon the appropriate course of action, applying sanctions where

Report to CEOP

Report to Child Protection team


Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experiences and practice as required
Provide collated incident report logs to LSCB and / or other relevant authority as appropriate
Await CEOP or Police response
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
If no illegal activity or material is confirmed then revert to internal procedures
Implement changes
Monitor situation
In thecae of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action