COUNDON COURT SCHOOL

E-SAFETY POLICY

AY2223

Agreed by Governors:	**September 2022**
Frequency of Review:	**Annually**
Date of Next Review:	**September 2023**

Contents

1. E-Safety Policy Statement

1.1 Coundon Court owes its staff and students a duty of care to provide safe use of its ICT systems and infrastructure. This policy reflects the need to raise awareness of the safeguarding issues associated with the use of digital technology and communications. E-Safety includes Internet and electronic communications together with the use of digital devices such as smartphones and tablet devices. It highlights the need to educate students and staff about the benefits and risks of using technology and provides safeguards and advice to mitigate the latter.

1.2 In developing this policy, Coundon Court has consulted with, and taken account of, guidance issued by the Department for Education; BECTA; JISC Legal Advisory Service and the Coventry City Local Safeguarding Children Board E-Safety Steering Group (LSCB).

1.3 The Policy will be:

1.3.1 Reviewed and monitored by the Principal.

1.4 The Leadership Team will receive an annual report on E-Safety from the Designated Safeguarding Lead which reports and reviews how all safeguarding duties have been discharged.

1.5 This policy is intrinsically linked to a number of other Coundon Court policies which are itemised in Section 8.

2. Managing E-Safety

2.1 The Principal is ultimately responsible for Coundon Court's safeguarding obligations. In practice, strategic and operational responsibility for E-Safety is delegated as follows:

2.2.1 Technology access, support, and security (all users) – Network Manager

2.2.2 Welfare and guidance (students) – Designated Safeguarding Lead 2.2.3

Welfare and guidance (staff) – Designated Safeguarding Lead

3. Purpose and Controls

3.1 World Wide Web

3.1.2 Purpose

- The purpose of World Wide Web use at Coundon Court is to enable flexible communication; promote learning and achievement by students; support the professional work of staff and to enhance Coundon Court's management and administrative functions.
- The World Wide Web is a valuable tool for students and staff; however, this entitlement is predicated by a requirement for all users to act responsibly within Coundon Court's policies and the law.

3.1.3 Controls

- World Wide Web access is filtered by an internally hosted and managed firewall service (*Smoothwall*) to ensure inappropriate, illegal, or unauthorised content is blocked.
- Drop-in computer use will be monitored from secure staff terminals using ***Impero Safeguarding*** software. When appropriate, screenshots will be captured to evidence inappropriate activity.
- Periodic network scans are run to ensure that inappropriate, illegal, or unauthorised content is not being stored on Coundon Court's systems.
- In the event that staff witness or have to record inappropriate activity, they will be offered pastoral support and access to appropriate professional support services.
- Staff are given clear guidelines to ensure that they do not unwittingly commit an offence while capturing and supporting evidence.
- Users are given clear objectives for internet use and expected behaviours.
- Users are educated in taking responsibility for their own internet access.
- Students will be taught ways to validate information by cross-checking before accepting its accuracy.
- Students will be made aware that the author of a web page, an e-mail or text message might not be who they claim to be.
- Users will be encouraged to inform a manager or member of staff immediately if they witness or are subjected to any content or activity that makes them feel uneasy or unsafe.
- Users will be encouraged not to divulge any personal or sensitive information, particularly through unsolicited requests.
- The CEOPS (Child Exploitation Online Protection Service) Report Abuse button is provided on the School Website.

3.2 Purpose

All users:

- Need to use e-communications as part of their learning or work.
- Staff should only contact students with their Coundon Court email account or messaging service for Coundon Court related communications.

- Staff should only contact students with their school mobile phone for Coundon Court related communications.
- Need to realise that this policy may also apply to any e-communication that they generate through any personal devices or accounts that they use.
- Should take care to use appropriate language when e-communicating with colleagues.
- Need to be made aware of the fact that once an email or text has been sent, it has been 'published' and cannot be retracted.
- Should avoid opening 'spam' messages, as these often contain inappropriate or malicious content.
- Will be encouraged not to divulge any personal or sensitive information, particularly through unsolicited requests.
- Will be encouraged to inform a manager or member of staff immediately if they witness or are subjected to any content or activity that makes them feel uneasy or unsafe.

3.2.1 Controls

- Coundon Court's staff email system is managed internally. Mail filtering. (SPAM) and virus checking is externally hosted by *Microsoft,* and managed internally by ICTS*.*
- The Coundon Court student email system is managed externally. Mail filtering (SPAM) and virus checking is externally managed by *Microsoft.*
- The Edulink messaging system is managed internally.
- Staff should be made aware that bullying can take place through E-Communication media out of Coundon Court, and the problems associated with this can manifest themselves in school time.

3.3 Social Networking and Web Technologies

3.3.1 Purpose

- Coundon Court encourages the appropriate and compliant use of Web technologies, whether hosted internally or externally.

3.3.2 Controls

- It is the responsibility of staff organising the use of such technologies to ensure use is in compliance with the law, and Coundon Court Policies and Procedures.
- All social Media sites are blocked by our firewall. Under circumstances where the curriculum or the business requires access to social media such as Facebook or Twitter, this can be managed and monitored by using ***LanSchool*** & Impero.

- Members of staff should not develop pages on Social Networking sites such as Facebook for students use, but instead should use the equivalent tools provided by the school's installation of Office 365 Teams or SharePoint.
- Where required Web functionality cannot be provided by internally hosted systems, or where awarding body requirements require use of a specific external service (e.g. Facebook), staff should seek permission prior to setting up any school-related activity on such systems. In such instances, we would require that any staff accounts are clearly identifiable as Coundon Court accounts. We would also require that privacy settings would be left sufficiently open to enable moderation of any activity.
- Before adopting the use of an externally provided Web service, the organiser shall appraise the stability and security of that service, the loss, damage and/or disruption that would be caused by failure of the service, and the corresponding benefit that using the service brings. IT Team should also be consulted to advice and security assessment.
- Web technology organisers must remind users of their legal obligations regarding Intellectual Property Rights, including copyright, prior to use of the technology.
- Web service organisers must consider the data protection aspects of their activity, and in particular, whether it involves the transfer of personal data out with Coundon Court systems. Personal data is any information which could be used to identify a particular person.
- Web service organisers must obtain the written permission of Coundon Court's data protection officer before any transfer of personal data to systems hosted outside of the European Economic Area.
- The Web service organiser must consider the accessibility issues inherent in the use of that technology, and consider, where appropriate, what equivalent learning experience could be offered to users unable to use the Web technology.
- Web technology organisers shall, upon becoming aware of potential liability attaching to the institution, remove the relevant item as soon as possible (or will apply to have the item removed as soon as possible).
- Staff should be aware that bullying and/or harassment can take place through social networking sites out of Coundon Court, and the problems associated with this can manifest themselves in school time.
- Users will be made aware that an online 'friend' might not be who they claim to be.

4 Computer Systems Security

4.1 The security of Coundon Court's computer systems will be reviewed regularly and subjected to regular internal audits.

4.2 Virus protection is managed internally through Anti-Virus products.

4.3 End users are responsible for ensuring their Portable media (USB drives etc) do not infect Coundon Court systems.

4.4 Portable media will be checked for viruses.

4.5 Staff should not be storing any ‘sensitive’ data outside of Coundon Court systems.

4.6 Any sensitive data that needs to be stored on portable equipment (e.g. laptop, USB drives and smartphones etc) must be encrypted using Coundon Court guidelines.

5 Risk Management

5.1 Coundon Court will take all reasonable precautions to ensure that users can only access appropriate content. However, due to the global and connected nature of Internet content, it is not possible to guarantee that unsuitable material will never be accessed via a school system. Coundon Court cannot accept liability for the material accessed, or any consequences resulting from Internet use.

5.2 Methods to identify, access and minimise risks will be revised regularly.

5.3 Staff, parents, governors and external advisors will work together to ensure that every reasonable precaution is being taken.

5.4 Students and staff will be informed that Internet and E-Communications use is supervised, monitored and, where appropriate, tracked.

5.5 All Internet access is filtered by an internally hosted Smoothwall firewall system.

5.6 If staff or students encounter unsuitable content or sites then these sites will be logged by the Smoothwall firewall system.

6 Reporting of Abuse and Incident Management

6.1 The school has published procedures for reporting cases of inappropriate activity and these apply equally to technology related incidents.

6.2 These procedures are issued to all members of staff and all new recruits to the school during their induction.

6.3 Learner-related e-safety incidents will be dealt with by Curriculum Areas and the Safeguarding Team.

6.4 Staff-related e-safety incidents will be dealt with by Departments and Human Resources.

6.5 Any subsequent action will be monitored via the relevant Coundon Court Policy referred to in Section 1 of this Policy.

7 E-Safety Training and Awareness Raising

7.1 E-Safety behaviours will be explained and discussed as part of the tutorial process.

7.2 An online E-Safety training course will be made available to all staff via iHasco & Sharepoint.

7.3 Acceptable Use of Coundon Court Computer Systems will be displayed in IT Classrooms.

7.4 A range of promotional media will be produced using clear and accessible language.

7.5 All staff will be made aware of this E-Safety policy.

8 Policy Umbrella

8.1 This is a subsidiary policy of the following:

PP Safeguarding Policy

8.2 This policy needs to be read in conjunction with the following policies and codes:

PP Anti-Bullying

PP Data Protection Policy

PP Employee Standards and Code of Conduct

PP Staff Code of Conduct