LAGAN COLLEGE BELFAST

E-Safety, ICT Acceptable Use and Digital Media Policy

Policy reviewed – May 2022

1 INTRODUCTION

This policy links with the United Nations Convention on the Rights of the Child (UNCRC) by taking into consideration the below articles of the UNCRC:
Article 19: Governments should ensure that children are properly cared for, and protect them from violence, abuse and neglect by their parents, or anyone else who looks after them.
Article 32: The government should provide ways of protecting children from work that is dangerous, or might harm their health or their education.
Article 36: Children should be protected from any activities that could harm their development.

1.1 What is the Internet, Cloud and Digital Media?

Internet – The internet is an electronic information highway connecting many millions of computers and individual subscribers all over the world. As this global network is not governed by an international body, there are obviously dangers concerning the kind of information that is accessible to its users. However, the educational value of appropriate use of information and resources located on the internet is substantial.

Cloud – Cloud based learning and teaching encompasses a broad range of educational resources available in an online environment. This includes My School, Google Classroom and other online resources.

Digital Media – This covers all hardware, software, portable and non-portable devices used for educational purposes inside and outside of school.

1.2 Rationale for pupil use of the Internet, Cloud and Digital Media

The school encourages pupils to use the rich educational information sources available on the internet and cloud, together with the development of appropriate skills using digital media to fully utilise such resources. Online resources offer pupils a broad range of up-to-date information; provide independent research facilities; facilitate a variety of learning styles; and encourage pupils to take responsibility for their own learning. E-literacy is a fundamental requirement for all pupils in order to prepare for the continually developing technological age that we live in.

1.3 Networked Access to the Internet, Cloud and Digital Media

The school provides filtered internet access to pupils and staff on both the C2k and the school's non-C2k networks. **Only filtered internet connections provided by, or on behalf of the school may be used to access on-line material at school.** Parents, pupils and staff are reminded that all mobile electronic devices must also be used in accordance with the mobile phone policy.

1.4 **How will pupils gain access to the Internet, Cloud and Digital Media at School?**

- During lCT lessons
- Through subject use across the curriculum
- During extra-curricular activities
- In the study areas, during normal school hours and occasionally at other times
- Through Wireless provision (filtered)
- Through use of iPads

1.5 Are there any dangers associated with using the Internet, Cloud and Digital Media?

Since the internet and cloud is composed of information from a vast array of sources worldwide, it includes some material that is not of any educational value in the context of the school. This material may include information that is inaccurate, abusive, profane, sexually oriented, racist or illegal.

In order to guard young people from any inherent dangers, it is the joint responsibility of the school and parents/guardians to educate pupils about their responsibility when using the internet and cloud.

1.6 Promoting Safe Working Practices

The school is determined to continue to provide high quality training for staff and pupils to make best use of its lCT facilities. Pupils will be provided with appropriate training and guidance on how to safely use the internet, cloud and digital media during KS3 lCT classes, PD Programme and assemblies. Staff will continue to receive appropriate training in the safe use of the internet, cloud and digital media. Pupils and staff will also be advised of the Health & Safety issues surrounding the use of digital media technology. *(Reference Section 13: E-Safety Practice)*

1.7 Promoting Awareness with Parents, Governors and Community

The school is committed to ensuring all stakeholders are made aware of this policy. The policy will be disseminated to parents, governors and staff. It will also be available on the school website so that other interested stakeholders can have full access. In addition, regular references will be made to the policy in communications with all stakeholders.

2 RESPONSIBILITIES OF STAFF AND PUPILS

2.1 Pupils are responsible for good behaviour when using the internet, cloud and digital media just as they are in the classroom or elsewhere in the school. All students are expected to adhere to the College's Student Expectations.

2.2 The school has a filtered internet, cloud and e-mail service. Pupils and staff will be made aware that internet, cloud and e-mail services are monitored and are not therefore private; internet, cloud activity and e-mail messages can be viewed by the Principal at any time. While normal privacy is respected and protected by password controls users must not expect internet and cloud activity, e-mail or files to be absolutely private.

Whilst access to the internet on the C2k and non-C2K systems is heavily filtered to protect the interests of staff and pupils, in certain circumstances access may be granted for staff to access sites which would normally be restricted. Requests for access to blocked sites should be made using the block site access from MySchool. In accessing these sites, staff should exercise caution. These sites may contain inappropriate or questionable information including user

generated content. It is the responsibility of staff who wish to use these restricted sites to suitably vet the links they plan to use.

2.3 Particular care should also be taken while projecting information from a digital media device onto a whiteboard or other form of facility, as inappropriate material may be displayed.

2.4 Access to the internet, cloud and digital media requires parental permission and a signed declaration by pupils agreeing to the College expectations for use of the internet, cloud and digital media.

2.5 The school will ensure that all pupils understand how they are to use the internet, cloud and digital media appropriately and why the rules exist.

2.6 The internet, cloud and digital media is provided for pupils to conduct research, communicate with others and fulfil their curricular requirements. While the use of information and communication technologies is a required aspect of the statutory Northern Ireland Curriculum, access to the internet, cloud, digital media and C2k NI services remains **a privilege and not a right**. Access is granted to pupils who act in a considerate and responsible manner, and will be withdrawn if they fail to maintain acceptable standards of use.

2.7 During school hours, teachers will guide pupils towards appropriate materials. Outside school hours, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, movies, radio, and other potentially offensive media. **Please note that any filtering available at home may not be subject to the same stringent requirements as we have in place to protect users at school. Additionally parents need to be aware of advertisements banners on sites; these may contain inappropriate materials.**

2.8 When using the internet, cloud and digital media at school, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws.

2.9 If at any time pupils find themselves able to access, internet sites which they think should be blocked, from within the school, they should advise their teacher immediately. Likewise, staff should immediately advise the member of a Senior Leadership Team.

2.10 Any resources or materials downloaded by teachers, pupils or parents for use within school, must abide by the requirements of this policy and be suitable for use in the classroom. If an individual is unsure regarding the appropriateness of content, they should seek advice from the member of the Senior Leadership Team before accessing the material within school.

2.11 All school resources (including computers, laptops, tablets and other digital devices) and their associated accessories are provided for educational use; they must not be used for any other purposes. Only portable resources may be removed from school, to facilitate preparation for teaching and learning; however, the resources may not be passed on to any third party.

3 EXAMPLES OF ACCEPTABLE AND UNACCEPTABLE USE OF THE INTERNET, CLOUD AND DIGITAL MEDIA

3.1 **Activities which are encouraged include, for example:**

- The use of digital media for appropriate educational purposes only to communicate between colleagues, between pupil(s) and teacher(s), between pupil(s) and pupil(s), between schools and industry;
- Use of the internet, cloud and digital media to research and develop topics related to social, personal, academic and professional development;
- Use of the internet, cloud and digital media to investigate careers, continuing professional development and Further/ Higher Education; and
- The continuing development of pupils' and staffs' ICT competence skills.

3.2 Activities which are <u>not</u> permitted include, for example:

- Retrieve, store, send, copy or display offensive information;
- Use obscene, racist or offensive language;
- Harass, insult, bully (cyber bullying) or cyber attack others;
- Share or use another user's password;
- Leave a computer unattended when it is logged on;
- Trespass in another user's folders, work or files;
- Intentionally waste resources (such as on-line time and consumables);
- Use the network for unapproved commercial purposes;
- Share information with others relating to another without their prior consent;
- Share intimate information or images about themselves or others;
- Use ICT resources in any way that contravenes Health & Safety guidelines;
- Search, download, view and/or retrieve materials that are not related to the aims of the curriculum or future careers;
- Damage any school device, computer system or computer network. This includes hardware, software, files or information stored/displayed on any school device;
- Load / connect any unauthorised outside software or hardware onto the school system;
- Spread computer viruses (all downloaded files and external storage devices must be checked for viruses before being used on the school system);
- Violate copyright laws -copy, save and/or redistribute copyright protected material;
- **Attempt to access the internet independent of the school's filtered C2K and non-C2K system. No other wireless or wired internet connected is permitted (including mobile internet);**
- Subscribe to any services or order any goods or services, unless specifically approved by the school;
- Play computer games or use interactive social media 'chat' sites, unless specifically assigned by the teacher;
- Use the network in such a way that use of the network by other users is disrupted (for example, downloading large files during peak usage times; sending mass email messages);
- Publish, share or distribute any personal data/information about a user (such as home address, email address, phone number etc.);
- Any activity that violates a school rule;
- Use any equipment to photograph, record or video any school activity for which explicit permission has not been given;
- Use or distribute, including on social networking sites, any material relating to school activities, pupils or staff for which explicit permission has not been given. This includes the posting of material, images or video footage relating to school staff, pupils, the school environment or school name without prior written consent from the Principal. This applies to curricular and extracurricular aspects of school life as well as to all school trips; and

- Engage in any activity that is harmful or hurtful to others.
- To access subscription video streaming service such as Netflix, Amazon Prime etc.

4 SANCTIONS

4.1 Violation of the above rules will result in a temporary or permanent ban on internet, cloud and digital media use. Additional disciplinary action may be added in line with existing school discipline policy rules on inappropriate behaviour. *(Reference CB Positive Behaviour Policy)* Where applicable, the PSNI or local authorities may be involved.

5 LOCATION AND PUPIL SUPERVISION

5.1 There is broad access to the internet, cloud and digital media covering most areas of the school including filtered wifi.

5.2 In order to reinforce good practice. It is important that pupils should frequently be reminded of their responsibility to use the internet, cloud and digital media in line with the school policy on acceptable use.

5.3 While using the internet, cloud and digital media at school, pupils should, where possible, be supervised directly by a member of staff.

6 STAFF USE OF INTERNET, CLOUD AND DIGITAL MEDIA

(Reference LCB Safeguarding Policy - Staff Code of Conduct)

6.1 Teacher use of the C2K service, non-C2K networks and digital media devices must be in support of the aims and objectives of the school curriculum and School Development Plan. C2k NI in particular supports the implementation and sharing of effective practices and collaborative networking across the province, as well as nationally and internationally.

6.2 The internet, cloud and digital media training of staff will also focus on the use C2K NI resources, amongst others, in their teaching and learning activities, to support the school's pastoral life and streamline administration procedures. Furthermore, staff will be given the opportunity to request additional training at any time.

6.3 All school staff (both teachers and non-teaching staff) are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the school.

6.4 **Staff must not communicate with pupils, either personally or professionally, using social networking sites, email or other technologies which are not managed or approved by the school or C2k providers**. Staff are advised that it is neither acceptable practice, nor school policy, to befriend or browse the profiles of pupils or parents using social networking sites e.g. Facebook. Similarly, it is not considered appropriate or acceptable for pupils or parents to request "friend" status with staff. It is not considered appropriate or acceptable for staff to take or distribute photos or video for the use on their personal social media sites. Furthermore, for both professional and personal security, staff are strongly encouraged to regularly review their own personal security settings on social media sites in line with similar advice and guidance provided for pupils annually. *(Reference LCB Safeguarding Policy - Staff Code of Conduct)*

All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, is still subject to copyright, data protection and Freedom of Information legislation. It is never considered acceptable behaviour for staff to reference school business, policy, practice or pupils via any social media unless through an officially created and maintained account.

6.5 It is the responsibility of the school network manager to ensure that, in the absence of available technical support, the integrity of the network is preserved to a level which safeguards both data and child protection procedures.

7 ACCEPTABLE USE OF DIGITAL MOVING/STILL IMAGES OF PUPILS

7.1 All staff should follow the guidance below when dealing with taking, display, storage and use of moving/still images of pupils.

7.2 **Taking of Photographs/Video of Pupils**

Parents will be asked to give their consent in writing to a range of such activities. A central database will be maintained of those pupils for whom parental permission has and has not been received. Staff will be required to consult this database prior to taking any images of pupils.

7.3 **Display/use of Photographs/Video of Pupils**

Staff are permitted to capture and/or use moving/still images of pupils, for whom parental permission has been appropriately received, for display purposes and publicity in and outside school, in school publications, on the school digital signage and website. It is not considered appropriate or acceptable for staff to take or distribute photos or video for the use on their personal social media sites. Where staff require additional guidance on the display/use of moving/still images of pupils, the Principal should be consulted. The Principal must grant permission for images of pupils to be distributed to any external media provider.

7.4 **Capture & Storage of Photographs/Video of Pupil**

Staff are encouraged to call upon the College's PR/Marketing Coordinator to assist with the taking of photographs/video for school business. It is recognised, however, that in many circumstances (for example, field trips, sporting events or incidental activities within departments) this is not always possible or appropriate. In these circumstances, staff are encouraged to capture moving/still images of pupils using hardware which has been procured by the school. It is not considered acceptable to use personal mobile phones to capture any such images. Furthermore, it should not be normal practice to store images of pupils (however obtained) on school/personal digital media devices, in a printed format or on any external memory device as a matter of course for prolonged periods of time.

As a result, staff should ensure that:

1. Any images of pupils stored digitally should be stored on C2K staff folders. Technical support will be available from the ICT support staff to assist in the transfer of existing/new images.

2. Staff must transfer digital media from capture devices to C2k staff folders at the earliest possible opportunity. In order to maximise the efficient use of school resources, staff should do this by ensuring that:
    - ONLY files which are most suitable for school business are selected
    - Selected files are copied to a shared C2K staff folder
    - Remaining images from the initial capture device are deleted
    - Images are located in an appropriately named folder.
    - (Consider *Activity Year Group -Date* to be appropriate, e.g. "Residential Y8 20.5.14")

3. Staff are discouraged from storing images of pupils on school provided portable devices; however, it is recognised that, to facilitate editing or selection this may be essential. In these circumstances, personal portable devices should not be used. It is expected that, after initial use by staff, digital images of pupils should be deleted from portable devices as soon as possible.

4. Staff should not pass images of pupils to third parties without consulting the Principal. Please consult the Principal if you require further advice.

Some subjects, for example drama, media studies and physical education, have specialist course requirements which necessitate the use of digital moving/still images of pupils to address course criteria. In some circumstances, technical limitations of the C2k NI system prevent files from being usefully stored within the staff resources area. In subjects where these circumstances have been identified, the storage of digital images is permissible on external storage (encrypted, if taken off site) devices providing:

1. The storage device is owned by the school.
2. The storage device is normally retained within the school building.
3. All departmental staff members are fully aware of the purpose of the specific storage device and its normal secure location within the school building.

There may be a need, at certain times throughout the year, to facilitate formative and summative feedback or assessment. In these circumstances, the storage device may be taken home by the staff member concerned providing:

1. All reasonable precautions are taken to ensure the security of the storage device.
2. The storage device is returned to school at the earliest opportunity.
3. The storage device is strictly used for purposes approved by the school only.
4. The storage device is encrypted with a password.

8 INFORMATION AND DATA MANAGEMENT

8.1 The school values the importance of appropriate data management procedures and practices and requires all staff to be prudent regarding sensitive personal materials, whether paper based or electronic.

Staff are encouraged to use SIMS.net to access the personal information of pupils. This is provided within school and is always password protected.
Staff must **not** store electronic copies of sensitive personal information on the following:

- Any personally owned portable or non-portable device.

- Portable storage devices eg. portable hard-drive or memory stick. (Neither School procured nor personally owned portable devices are considered acceptable for sensitive data).

Staff may store basic pupil information electronically, for example, name, form class and performance statistics, for the purposes of recording pupil achievement throughout the year. This information may be removed from the school building to facilitate assessment activities. Staff must ensure that they hold the minimum amount of personal data necessary to enable them to perform their duties. The data must not be held any longer than necessary for the purposes it was collected for. Every effort must be made to ensure that data is accurate, up to date and that inaccuracies are corrected without any unnecessary delay. Staff are advised to be prudent about the sensitivity of this data and are required to maintain its confidentiality.

9 PERMISSION FROM PARENTS AND GUARDIANS

9.1 Parents/guardians will be provided with the e-Safety, ICT Acceptable Use and Digital Media Policy and permission will be sought for their child/ren to use the internet, cloud and digital media. Pupils are also required to sign an undertaking agreeing to their proper use of the internet, cloud and digital media. Details of the letter sent to parents and additional guidance information is included in the appendices to this policy.

10 WEBSITE & DIGITAL SIGNAGE

10.1 The school website and digital signage will be supported by the ICT Support Team and updated and monitored by a range of staff member.

11 USE OF SOCIAL MEDIA SITES FOR EDUCATIONAL PURPOSES

11.1 Subject to the approval of the Principal, staff may use social media sites for educational purposes only.

Staff requesting the use of such sites for educational purposes must:

- Specify the proposed site;
- Specify who would be involved;
- Conduct a risk assessment;
- Provide a clear rationale stating the benefits of the proposed activity; and
- State how long the site will be operational.

Only one member of staff should be responsible for the operation of the site. Their login and password details must not be shared. Another nominated member of staff should be responsible for the frequent moderation of the site. This will normally be the relevant Head of Department. The social media site must only be used for educational purposes strictly related to the topic(s) being covered. Any breech of this or unacceptable behaviour may result in the user being denied any further access to the site. The user will be subject to any appropriate disciplinary procedures in line with the school's Positive Behaviour policy and the E-Safety, ICT Acceptable Use and Digital Media Policy.

Approval must be sought from the parents/guardians of any pupils who may be using the site before access is granted.

12 BRING YOUR OWN DEVICE (BYOD)

12.1 The use in school of devices owned personally by staff and pupils is subject to the same regulations/rules as if they were provided by the school.

Please note: Some devices may not be suitable for use on the school network. The school cannot guarantee connectivity or the quality of the wifi connection with personal devices.

The user/owner of a device being connected to the school network should adhere to the following conditions:

1. The device must be used in accordance with the e-Safety, lCT Acceptable Use and Digital Media Policy.
2. Any inappropriate content stored on the device in breach of the e-Safety, lCT Acceptable Use and Digital Media Policy must be removed before it is brought into the school premises.
3. An up-to-date anti-virus/internet security product must be installed on the portable device or external storage device.
4. As the school's insurance does not cover personal devices used in school, appropriate insurance measures should be in place to cover the device for this application.
5. As devices may have a tracking facility, it would be advisable to have it enabled when being used in school to assist in the relocation of the device if lost or stolen.
6. **The school accepts no responsibility for any privately owned devices brought into school. Pupils/staff are solely responsible for the safety (including content) of devices on their way to school, during school and on the return from school. It is the responsibility of pupils/staff to look after their own personal devices and therefore they should keep the devices with them at all times. The school is in no way responsible for personal devices that are broken, lost or stolen while at school or during school activities.**
7. Use of the internet, cloud and email is monitored and any use that is deemed to be inappropriate will be reported to the Principal. The Principal can request internet, cloud and email usage log for all users at anytime.
8. Devices may be checked at any time for inappropriate use.
9. If a student or member of staff finds inappropriate and/or illegal materials available on their device, the Principal should be informed immediately, giving details of their name, inappropriate material, time and date of incident.
10. There should be no use of camera facilities (if available on the device) to take images! video of pupils or staff without permission.
11. **Users who wish to connect their personal equipment to the school wireless network should have no expectations of hardware or' software support from the school**
12. **Devices should be named ideally with a UV pen in accordance with advice from the police.**
13. **Pupils and staff will be responsible for the security and protection of their passwords and if a device is left unattended the user should have either *logged* off or locked the device to prevent anyone using it in their absence.**
14. All use of the Internet is governed by a legal agreement with our Internet Service Provider (ISP).

15. If a user suspects that their device has been affected by a virus or other malware, it should be removed from the school network and fixed before using it on the school network again.
16. Personal devices should not be connected to the school's peripherals, eg. printers.
17. Devices must be in silent mode while in school, unless otherwise allowed by a teacher.
18. Printing from personal devices may not be possible (Pupils are not permitted to bring their own personal printing devices).
19. Pupil owned personal devices should be charged before school and should run on battery power while at school.
20. Portable devices/electrical items owned by staff members or pupils are not to be brought into the school unless they have a current Portable Appliance Testing (PAT) Test Certificate (i.e. within the last 12 months). In all instances, the school is to be made aware of the intention to use 'private' electrical equipment in the School.
21. The school is in no way responsible for the maintenance of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).
22. Filtering may not block all inappropriate content.
23. Internet access can be removed for individuals and appropriate sanctions applied.
24. Pupils and staff should be conscious of personal safety when carrying devices to/from and around school
25. Pupils and staff should be conscious of personal safety when communicating on-line, and therefore must not share unnecessary personal information about themselves or others.
26. The school reserves the right to withdraw permission, at any time, to allow any individual to use personal devices in school.

We hope that following these instructions will help to make the use of ICT a positive experience for both our pupils and staff.

13 E-SAFETY PRACTICES

13.1 This section provides a set of guiding principles for keeping pupils and the wider college community safe online and for prioritising online safety within the school's preventive education curriculum and overall Safeguarding policy.

In Lagan College, online safety for students, staff and the wider community is a paramount concern. Lagan College wants pupils to have the opportunity to avail of all the positive benefits that come from learning, exploring and connecting with each other online. However, in doing so, they need to know how to protect themselves. It is important that students understand the impact of their behaviour when engaging with online technologies and how to act appropriately and stay safe

13.2 KEY FEATURES OF LCB ONLINE SAFETY PRACTICE

Key Feature	Practice	Resources
Online safety forms an integral part of the school's safeguarding/child protection policy and is approved and monitored by the Board of Governors	• To ensure online safety is referenced in relevant policies: • Behaviour • Anti-Bullying Policy • Safeguarding Policy • Staff Code of Conduct • CP Training for Governors includes E- Safety procedures • Governors are consulted in drafting and revising policy • INSET Staff training and register of training • Signed contracts/agreements in Student Learning Planners and Policies	Code of Conduct for Staff Annex C 2017/04 School Policy DE 2016/27, DE 2016/26 E-Safety, ICT Acceptable and Digital Media Policy Anti-Bullying Policy Safeguarding Policy Staff Code of Conduct INSET Training resources
Key Feature	Practice	Resources
Policy and procedures about online safety are integrated into existing safeguarding/child protection, behaviour, code of practice, anti-bullying policies	• Relevant policies must be revised following DE 2016/26 Practice • Clear Practice in policies outlining relevant aspect of online safety	DE 2016/27, DE 2016/26 E-Safety, ICT Acceptable and Digital Media Policy Anti-Bullying Policy Safeguarding Policy Staff Code of Conduct
Key Feature	Practice	Resources
There are clearly defined procedures for reporting and dealing with incidents surrounding breaches in the school's online safety guidelines	• Procedures for reporting clearly outlined in E-Safety, ICT Acceptable and Digital Media policy • Implicit Staff, Student and Parental training and updates each year in August and September • Procedures are shared with students, parents and staff in Student Learning planner and on website • College will make PSNI aware of any at risk online safety issues	Securus (To be implemented Term 3) PSNI Leaflets Think You Know website Online Safety Risk Register ipad Health Checks
Key Feature	Practice	Resources
E-Safety, ICT Acceptable and Digital Media Policy The online safety section incorporates agreements on the acceptable use of: the Internet and school-based Digital Technology. Personal Mobile Technology	• Policy and agreements must follow Practice from DE 2016/26 • Acceptable Use must be reviewed annually • School policy should include rationale for use of internet, digital and personal mobile technology • Policy should outline how internet access is regulated • BYOD policy should incorporate DE 2016/26 • Students should be made aware of sexting and inappropriate use of personal mobile technology • Staff use of internet, cloud and digital technology must be incorporated to agreements	Use of Jamf LCB Assembly programme, PPTs
Key Feature	Practice	Resources
A Consistent Whole School Approach	• Staff training clearly outlines school approach to online safety and use of digital technologies	Online safety calendar RT Social Media C2K homepage Practice

	• Vice Principal (Pastoral) is responsible for delivery of online safety to staff • *There is Key Stage development across the curriculum including online mapping* • *Online safety development should be included in school action plans* • Sharing of best practice should take part on staff training days and collaboratively across EBALC	EBALC online safety sessions VP Pastoral is CEOP trained INSET Training resources
Key Feature	Practice	Resources
Staff Education	• Planned staff training as part of staff development programme on appropriate use of social media and online safety, child protection and safeguarding • Sharing updates with staff throughout the year • Higher level training DT staff such as CEOP	Legal Island CEOP training materials 360 Safe VP Pastoral and Sharon McKee – CEOP trained
Key Feature	Practice	Resources
Education of Pupils	• Use of assemblies • Posters, noticeboards and school website • Planned delivery across the curriculum in PD, LLW, ICT, Pastoral Programme The PD Programme is flexible, relevant and engages pupils' interest; e-safety is promoted through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. • Positive rewards are used to cultivate positive and responsible use of digital devices • Peer mentoring programmes. • Use of outside agencies such as C2K • Participation in events such as Safer Internet Day and competitions by C2K/EA • Collaborative work through Shared Education and EBALC • Student led initiatives such as Digital Leaders / Ambassadors / peer learning	Website has link to CEOP CEOP link JamF Where is Klaus? Can I be your friend? Assembly scripts PD E-Safety module
Key Feature	Practice	Resources
Education of Parents and Wider Community	• Annual Parental information sessions on online safety • Publication of practice and policy to parents • Updates and new resources shared through 'update emails' and the school website for parents and wider community • Maximise use of planned events throughout the year to promote online safety • Student led initiatives such as Digital Leaders / Ambassadors / peer learning	PPT Parental E-Safety Emails to parents on emerging apps that may put students at risk

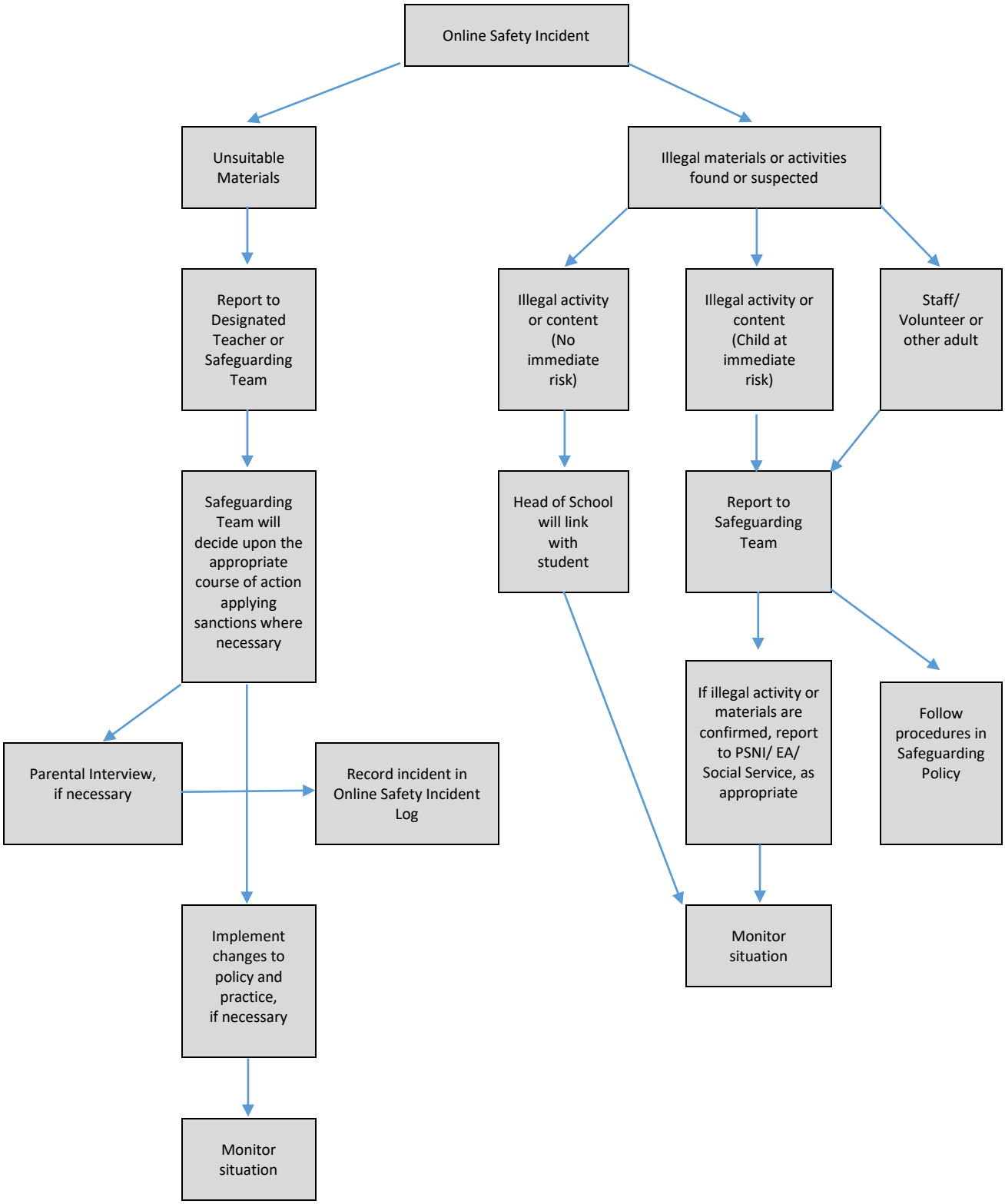
Key Feature	Practice	Resources
Monitoring and Evaluation	• Schools maintains an Online Safety Risk Register • Principal regulates SIMS access levels for staff • Risk assessment has been completed and used to promote E-safety. • Data is used effectively to assess the impact of e-safety practice and how this informs strategy. • Use of JamF is monitored by IT • ipad Health Checks	kidscape.org.uk Risk Assessment Online Safety Risk Register https://360safe.org.uk/Overview https://swgfl.org.uk/products-services/online-safety/resources/online-safety-policy-templates/
Key Feature	Practice	Resources
Management of Personal Data	• Schools follow Practice on handling personal data from the Data Protection Act 1998, Freedom of Information Act 2000 and upcoming GDPR 2018 • Schools should communicate clearly and professionally at all times when using technology • Transfer of data should follow advice outlined in DE Circular 2015/21 • Personal data should be kept on a secure server	https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf
Key Feature	Practice	Resources
Reporting	• Clear Practice and instructions are given to staff, students and parent on reporting online safety concerns • Procedures to manage an online safety incident are clearly set out. • Procedures are set out to students via the school website, student learning planner and PD programme • Incidents relating to child protection are reported to the designated teacher/ Safeguarding Team	IPads are monitored by IT and any issues reported to Designated Teacher to action. CP Reporting Form

13.3 CATEGORIES OF POTENTIAL ONLINE SAFETY RISKS

Students have a right to be protected and educated on now to keep safe online. Through the preventive curriculum, assembly and personal development programmes, the College aims to protect children and minimise the associated risks around online safety. These risks have been defined under three categories:

Risk	Definition	Commercial	Aggressive	Sexual	Values
Content Risk (child as recipient)	The child or young person is exposed to harmful materials.	- lifestyle websites, for example pro-anorexia, self-harm or suicide sites - advertisements - spam - sponsorship - personal information - misleading information or advice	- ignoring age ratings in games (exposure to violence, often associated with racist language); and substance abuse - hate sites - violent/hateful content	- Exposure to inappropriate content, including online pornography or unwelcome sexual content;	- Content validation: how to check authenticity and accuracy of online content - Bias - Racist
Contact Risk (child as participant)	The child or young person participates in adult- initiated online activity and/or is at risk of grooming.	- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords - Tracking - harvesting personal information	- Cyber-bullying in all forms - being bullied, harassed or stalked	- meeting strangers - being groomed	- self-harm - unwelcome persuasions
Conduct Risk (child as actor)	The child or young person is a perpetrator or subject to bullying behaviour in peer-to- peer exchange and/or is at risk of bullying, entrapment and/or blackmail.	- Copyright (little care or consideration for intellectual property and ownership – such as music and film). - illegal downloading - hacking - gambling - financial scams - terrorism	- bullying or harassing another	- creating and uploading inappropriate material; sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)	- privacy issues, including disclosure of personal information - providing misleading info and advice - health and well-being (amount of time spent online (internet or gaming)) - digital footprint and online reputation

13.3 MANAGING AN ONLINE SAFETY INCIDENT



This policy will be reviewed and updated as required.

APPENDIX 1: Additional Advice for Parents with Internet access at Home

1. The device with Internet access should be situated in a location where parents can monitor access to the Internet. Devices should be fitted with suitable anti-virus, anti-spyware and filtering software.
2. Parents should agree with their children suitable days/times/durations for accessing the internet.
3. Parents should discuss with their children the College expectations for using the internet, cloud and digital media and implement these at home. Parents and children should decide together when, how long, and what comprises appropriate use.
4. Parents should get to know the sites their children visit, software/apps they use and talk to them about what they are learning.
5. Parents should consider using appropriate internet filtering software for blocking access to unsavoury materials. Further information is available below.
6. It is not recommended that any child under 16 should be given unmonitored access to social media or chat facilities.
7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the internet, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.
8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such messages or images. If the message comes from an internet service connection provided by the school or by C2k, they should immediately inform the school.
9. Please note for your own information that many social networking sites have a minimum age restriction. In the case of Facebook, for example, the recommended age for use of this site is 13 years of age.

Further free advice for parents is available from the following sources:
http://www.thinkuknow.co.uk/ - A website designed to inform children and parents of the potential hazards involved with online chatrooms.

http://www.parentsonline.gov.uk/ - Promotes home school links by helping parents understand the role of Information Communications Technology (ICT) in learning. www.kidsmart.org.uk

http://www.wiseuptothenet.co.uk/ - The Home Office guide to Internet safety with downloadable leaflets for parents

http://www.getnetwise.org/ - Information about filtering programs for home use

Protecting Your Home Computer
To protect you home computer, parents are advised to ensure the following items of software are installed on their home computers:
Anti-Virus / Internet Security, Filtering and Anti-Spyware Software.