LINTON
VILLAGE COLLEGE

E-SAFETY

POLICY

Authors:	TD & SM
Group:	LVC Full Governing Body
Date Written:	January 2018
Last Review:	February 2020

Contents

Introduction

The use of technology is becoming a significant component of everyday life. Whilst this brings about many benefits that support students' ability to become independent learners, this presents the College with an ever-increasing number of challenges to ensure that this technology is used responsibly. Technology often provides a platform that facilitates harm, such as: Child sexual exploitation; radicalisation and sexual predation. Linton Village College fully recognises the responsibility it has under Section 175 of the Education Act 2002 and Keeping Children Safe in Education 2016 to have arrangements in place to safeguard and promote the welfare of children. Furthermore, in the ever-changing landscape of the digital world, the College seeks to work in partnership with all stakeholders to ensure a consistent approach to e-safety.

The breadth of issues classified within e-safety is considerable, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful online interaction with other users;
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; and
- Commercialism: being exploited by hidden costs in apps, games and websites, as well as advertising through spam and pop-ups.

This policy sets out clearly and simply the principles, methods and monitoring systems which work together to seek to ensure that staff and students at Linton Village College are safe and secure when using technology. It also seeks to outline how staff and students can identify, intervene and escalate any incident that is linked to membership of the College.

This policy applies to all members of the College community (including staff, students, governors, volunteers, parents/carers, visitors and community users) who have access to and are users of College ICT systems, both in and out of the College.

There are two main strands to the College's e-Safety policy; these are:

- Protection,
- Education & Training.

Roles and Responsibilities - Protection

The College believes that Safeguarding is everyone's responsibility. Collectively, we have duty of care for e-safety and everyone has their role to play in this.

The Principal will

- Ensure duty of care for the safety (including e-safety) of members of the College community, though the day-to-day responsibility for e-safety will be delegated to the Safeguarding Team.
- Delegate responsibility for overseeing the College IT system to a member of the Senior Leadership Team – the SLT ICT Lead.
- Follow set procedures in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and the College disciplinary procedure).
- Regulate the behaviour of students, where reasonable, when they are off the College site, as stated in The Education and Inspections Act 2006 in line with the Behaviour and Discipline Policy.
- Empower members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the College, but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data in line with the Behaviour and Discipline Policy.

The SLT ICT Lead will

- Liaise with the Safeguarding Team to develop approaches to the protection of the College community.
- Meet regularly with the IT Support Team to review and refine the College infrastructure, with a particular focus on filtering and monitoring.
- Investigate any incidents of misuse of the College IT systems and follow-up in accordance with the College Behaviour and Discipline Policy, communicating with parents/carers and outside agencies as appropriate.
- Investigate any inappropriate use of e-technologies (e.g. Social media, apps, games) that impacts upon the College community and follow-up in accordance with the College Behaviour and Discipline Policy, communicating with parents/carers as appropriate.
- Coordinate the e-safety curriculum provision alongside the PSHE Team and Head of Computing – ensuring relevance, breadth and progression.

The Safeguarding Team will

- Take day-to-day responsibility for e-safety issues and take a leading role in establishing and reviewing the College e-safety policies/documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Ensure that the College is compliant with any current national e-safety guidelines.
- Provide appropriate training and advice for staff.
- Liaise with the Safeguarding Governor, the Deputy Principal or external agencies, as appropriate.
- Present termly reports to the Senior Leadership Team and Local Governing Body (Standards) that contain details of e-safety incidents and actions.
- Record incidents to inform future e-safety developments.
- Be aware of the potential dangers and challenges of safeguarding and child protection issues arising from:
  - sharing of personal data;
  - access to illegal/inappropriate materials;
  - inappropriate on-line contact with adults/strangers
  - potential or actual incidents of grooming;
  - cyber-bullying.
- Provide parents/carers with opportunities to learn about and understand current e-safety issues. For example through e-safety information evenings, the Linton Village College Newsletter, the College Website or National/local campaigns.

The IT Support Team must

- Take all appropriate measures to ensure that the College's technical infrastructure is secure and is not open to misuse or malicious attack.
- Advise SLT of any technical upgrades required to meet national guidelines, with associated costs and implications.
- Ensure that users may only access the networks and devices through a properly enforced password protection protocol.
- Apply appropriate filtering and monitoring to different user groups and update these on a regular basis.
- Keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- Regularly monitor the whole College network and report any misuse immediately to SLT.

- Maintain user internet logs for a 180 days.

All Staff must

- Have an up to date awareness of e-safety matters and of the current College E-safety Policy and practices.
- Have read the Code of Conduct for All Adults, in line with their safeguarding training.
- Report any problems with hardware immediately to the IT Technical Support team, using itsupport@lvc.org.
- Alert SLT and IT Technical Support team of any suspected misuse or vandalism for investigation and repair.
- Ensure that all digital communications with staff/students/parents/carers should be on a professional level and only carried out using official College systems – please refer to the Home College Communications and Internal Communication policies.
- Educate students on how to use technology appropriately and safely.
- Ensure that students understand and follow relevant sections of the e-safety Policy, and other policies relevant to the use of technology.
- Enforce all policies to ensure students remain safe and secure when using technology.
- Check that all research-based lessons are prepared to ensure that all sites are accessible to students.
- Report any unsuitable material that is found in internet searches, or site accessed, to the IT Support Team and SLT ICT Lead/Safeguarding Lead.
- Check that student access to planned searches on research topics (e.g. racism, drugs, discrimination) will not be blocked by the College's filtering system through liaison with the SLT ICT Lead and IT support. In such a situation, staff can request that these sites be temporarily removed from the filtered list for the period of study.

The Governing Body will

- Do all that they reasonably can to limit students' exposure to the four areas of risk – content, contact, conduct and commercialism – by ensuring that appropriate filtering and monitoring systems are in place.
- Review the effectiveness of the policy through regular updates from the safeguarding lead this will be carried out by the governors/LGB Standards committee receiving regular information about e-safety incidents and monitoring reports. The safeguarding governor will oversee all e-safety issues.

Students must

- Read and sign the code of conduct for the use of technology in their planners. (see appendix)
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understand the importance of adopting good e-safety practice when using digital technologies out of College and realise that the College's e-safety policy covers their actions outside the College day where this impacts upon the College community.

Parents/Carers should

- Ensure that they safeguard their children through the use of appropriate parental controls/settings on devices and internet access. This includes ensuring that all apps accessible to their children are age-appropriate.
- Work in partnership with the College to provide their children with a consistent understanding of e-safety based around the four Cs.
- Monitor their child's online presence, reporting any inappropriate content to the appropriate body and alert the College of any concerns that may impact on the College community.

Furthermore, parents/carers should also follow the guidelines below on their own appropriate use of:

- Digital and video images taken at College events may only be shared privately, with explicit permission from other students' parents/carers.
- Social media - should not be used to air grievances about the College or staff.

Visitors should

- Read the agreement on the use of their personal devices whilst on the College site upon signing in at reception.

Roles and Responsibilities – Education & Training

Whilst regulations and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of the College community in e-safety is therefore an essential part of the provision. All stakeholders need the help and support of the College to recognise and avoid e-safety risks and build their resilience.

Safeguarding Team and SLT ICT Lead must

- Work collaboratively to develop approaches to the education of the College community.
- Keep up-to-date on National and local e-Safety developments.
- Ensure that all stakeholders understand the four Cs of e-Safety through appropriate training opportunities and information updates.
- Provide an e-safety curriculum as part of Computing and PHSE lessons.
- Consult all stakeholders about the College's e-safety provision.
- The Safeguarding Team will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations. They will provide advice/guidance/training to individuals as required.

Staff/Volunteers must

- Reinforce key e-safety messages as appropriate across the curriculum.
- Teach students how to use technology safely, within the context of the lesson or series of lessons;
- Guide students to sites checked as suitable for their use, when planning the lesson, and that any unsuitable material that is found in internet searches is reported immediately to the IT Support Team.
- Receive e-safety training as part of their induction programme, ensuring that they fully understand the College e-safety policy.
- Attend annual refresher training in safeguarding and child protection
- Act as good role models in their use of digital technologies, the internet and mobile devices;
- Be vigilant in monitoring the content of the websites when students are allowed to freely search the internet.
- Educate students on the dangers of technologies that maybe encountered outside the College – both as part of the e-safety curriculum and informally when the opportunities arise.

- Make students aware of the impact of cyberbullying and how to seek help if they or their peers are affected by any form of online bullying.

Students will

- Read and sign the code of conduct for the use of technology in their planners.
- Take care when using the internet for research activities and use safe and effective retrieval skills to select appropriate content.
- Gain knowledge and understanding of how to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Appreciate how to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Have opportunities to develop resilience to radicalisation through a safe environment that enables them to debate controversial issues and understand how they can influence and participate in decision-making.
- Take responsibility for and report any form of cyber-bullying they encounter or become aware of.
- Be aware of where to seek help or advice if they experience problems when using the internet and related technologies; i.e. Parent/carer, teacher/trusted staff member, or an organisation such as Childline or CEOP report abuse button.

Parents/Carers

We recognise that some parents and carers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The College will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities,
- Letters, newsletters, web site,
- Parents/Carers evenings,
- High profile events/campaigns e.g. Safer Internet Day,
- Reference to the relevant web sites/publications, e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links/resources).

Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any subcommittee involved in technology/e-safety/health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation.
- Participation in College training or information sessions for staff or parents (this may include attendance at assemblies/lessons/meetings).

Technical – infrastructure/equipment, filtering and monitoring

The College will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will be effective in carrying out their e-safety responsibilities:

- College technical systems will be managed by the IT Support Team in ways that ensure that the College meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of College technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- 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 IT Technical Support team who will maintain the record of users and their usernames. Users are responsible for the security of their username and password.
- The IT Technical Support Team is responsible for ensuring that College-purchased software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations and any concerns are reported to SLT.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by actively employing a black list provided by Shalla. Content lists are regularly updated and internet use is logged and regularly monitored. All requests for filtering changes should be approved by the SLT ICT Lead.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet in line with The Prevent Duty 2015.
- The College has provided differentiated user-level filtering for different user groups of staff and students.

- IT Support regularly monitor and record the activity of users on the College technical systems and users are made aware of this.
- Any issues with any actual/potential technical incident/security breach are to be reported to via staff to the IT Support Team using ITsupport@lvc.org.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc… from accidental or malicious attempts which might threaten the security of the College systems and data. These are tested regularly. The College infrastructure and individual workstations are protected by up to date virus software.
- Any trainee teachers or long term supply will be granted temporary access to the College systems via an account, set up for the duration of their stay. Their personal devices may be connected to the Staff Wireless Network for the duration of their stay.
- Any other "guests", such as visitors or supply teachers, of the College will not have access to the College systems, although they may be allowed internet access via the "guest network".
- Any staff are able to download executable files and install programmes on locally onto their staff laptop.

Mobile Devices

Mobile devices may be College or personally owned and might include: smartphones, tablets, notebook/laptop or other technology that usually has the capability of utilising the College's wireless network. All use of personally owned devices are covered by the College's Personal Mobile Devices Policy.

Teaching about the safe and appropriate use of mobile technologies is an integral part of the College's E-safety education programme.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents/carers will be obtained before photographs of students are published on the College website/social media/local press.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at College events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images. Ideally those images should only be taken on College equipment, however when personal devices are used they should be deleted from the device as soon as they are posted online or transferred to the College network.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;

- Processed in accordance with the data subject's rights;
- Secure;
- Only transferred to others with adequate protection.

Social Media - Protecting Professional Identity

The College has a duty of care to provide a safe learning environment for pupils and staff. The Colleges could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the College liable to the injured party. Reasonable steps to prevent predictable harm are in place.

The College provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the College through:

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Risk assessment, including legal risk

College staff should ensure that:

- No reference should be made in social media to students, parents/carers or College staff.
- 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.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The College social media accounts will be used for sharing information about events relating to the College and it's community, as well as celebrating achievements and successes.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the College or impacts on the College, it must be made clear that the member of staff is not communicating on behalf of the College with an appropriate disclaimer. Such personal communications are within the scope of this policy.

- Personal communications which do not refer to or impact upon the College are outside the scope of this policy.
- Where excessive personal use of social media in College is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The College permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the College
- The College should effectively respond to social media comments made by others.

The College's use of social media for professional purposes will be checked regularly by Safeguarding Team and SLT ICT Lead to ensure compliance with the College policies.

Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from College and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a College context, either because of the age of the users or the nature of those activities.

The College believes that the activities referred to in the following section would be inappropriate in a College context and that users, as defined below, should not engage in these activities in, or outside, the College when using College equipment or systems. The College policy restricts usage as follows.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to the following:

- Unacceptable and illegal activities:
    - Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.
    - Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
    - Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008.

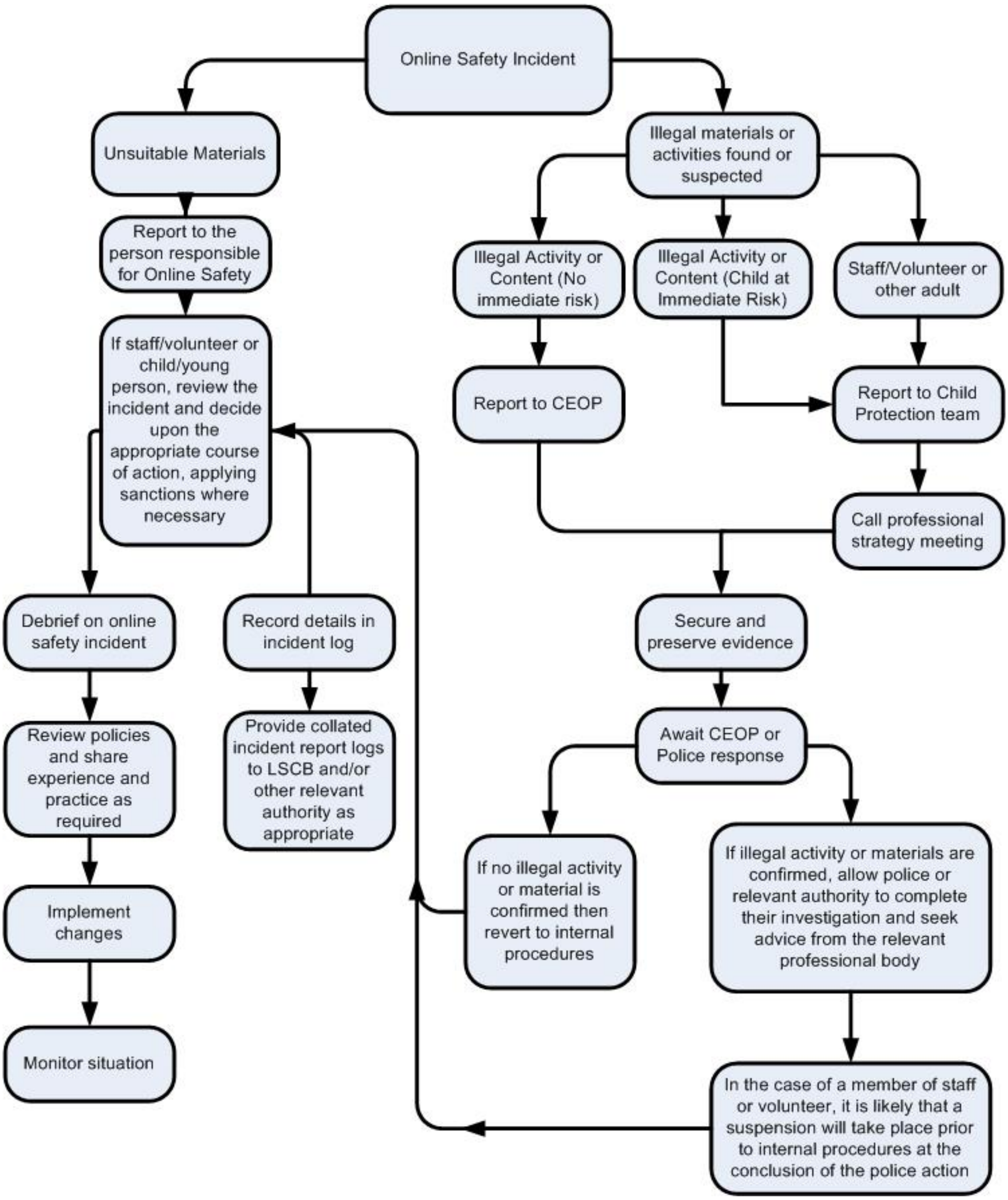
  - Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986.
- Unacceptable activities:
  - pornography;
  - promotion of any kind of discrimination;
  - threatening behaviour, including promotion of physical violence or mental harm
  - promotion of extremism or terrorism;
  - any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute.
  - using College systems to run a private business;
  - using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the college.
  - infringing copyright;
  - revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords);
  - creating or propagating computer viruses or other harmful files;
  - unfair usage (downloading/uploading large files that hinders others in their use of the internet);
  - on-line gaming (non-educational);
  - on-line gambling;
  - on-line shopping/commerce;
  - file sharing;
  - use of personal social media;
  - use of messaging apps.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to e-safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case 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

Other Incidents

It is hoped that all members of the College community will be responsible users of digital technologies, who understand and follow College policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the College and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The complete paperwork should be retained by the group for evidence and reference purposes.

Appendices

Code of Conduct & e-Safety (in student planner)

Introduction

At Linton Village College, we aim to educate and protect you in your use of technology. The use of the latest technology in your lives is growing rapidly, but with its use comes responsibility, in particular to protect both yourselves and the College from abuse of these technologies. This guide covers the use of all electronic devices within the College, irrespective of who the owner is.

The College accepts no responsibility for any mobile technologies brought in and those who choose to bring them into the College are responsible for them and bear the responsibility for any losses.

Mobile phones and other electronic devices will not be allowed to be seen, heard or used on the College site between 8:30am and 3:05pm. This includes all devices that have the ability to connect to the internet, send or receive any type of message, or play music or games, including smart watches.

Using the College's Equipment and Network

When using the College's ICT equipment you must use it responsibly and treat it with respect. You are expected to report any damage or missing/loose connections immediately to a member of staff.

You must use the internet in a responsible manner and take care to keep yourself and others safe. The College uses a filtering system to protect you from inappropriate materials.

You must not make any attempts to bypass this or any other security measures in place on the network. The College monitors and logs use of the network, including the internet, and your personal file space. You may use your personal area for storing any files that are directly related to your work in College.

Remember, you are responsible for keeping your passwords safe and when using your College email account you are representing the College community. All electronic communication must be polite and professional. You should always keep personal details private so that you are not easily identifiable by others and remain safe.

You must report any abuse, misuse or access to inappropriate materials to a member of staff immediately. You can do this in person, by emailing thinkpink@lvc.org or by completing a ThinkPink Peer postcard or contacting a member of the Safeguarding Team - Mrs Matarazzo, Mr Farr or Mrs Addley.

When carrying out research, it is important to reflect upon the sources you are using and not attempt to pass off others' work as your own.

Student

I understand that my parents may be informed if I misuse the College network or the internet. I have read this guide and understand that full details can be found in the College's Mobile Device Policy and e-Safety Policy, located on the College Website.

I recognise the need to swiftly report inappropriate activity to the relevant organisation, e.g. the website/app provider, the police or possibly the College if this activity is likely to impact upon the safety and/or well-being of a child at the College.

Student: _________________________________ Date: ________________

Parent/Carer

I/we understand the information provided in this guide, and that full details can be found in the College's Mobile Device and e-Safety policies, located on the College Website.

I/we acknowledge that it is my/our responsibility to monitor the apps and websites that my child accesses outside of College and to ensure they are age-appropriate

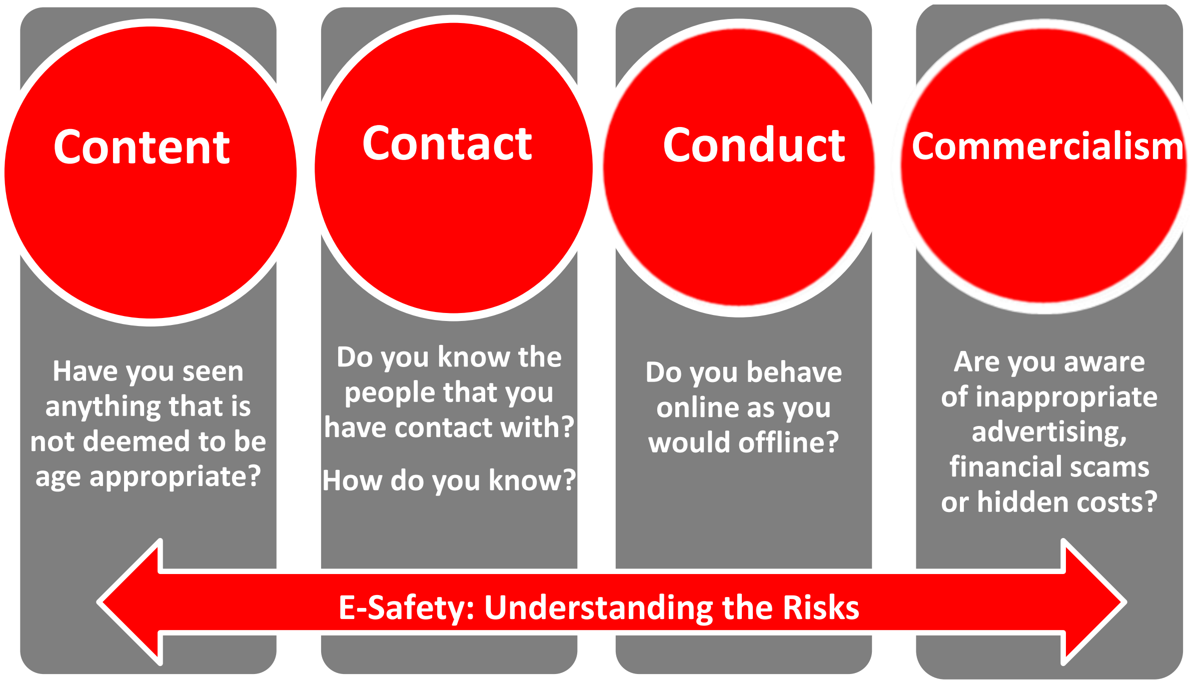
I/we understand that it is my/our responsibility to encourage moderate and responsible use of devices and technology.

I/we recognise the need to swiftly report inappropriate activity to the relevant organisation, e.g. the website/app provider, the police or possibly the College if this activity is likely to impact upon the safety and/or well-being of a child at the College.

Parent/Carer: _________________________________ Date: ________________

e- safety:

At Linton Village College, we use the 4 Cs to educate all stakeholders in e-Safety. This is an easy way for everyone to understand the risks associated with the internet and wider use of technology. At our e-safety evenings, parents/carers have often asked us how they can have meaningful and impactful discussions with their children around technology; we find that the 4 Cs, along with the questions beneath them, provide a useful prompt for these conversations.



Content

Have you seen anything that is not deemed to be age appropriate?

Contact

Do you know the people that you have contact with?

How do you know?

Conduct

Do you behave online as you would offline?

Commercialism

Are you aware of inappropriate advertising, financial scams or hidden costs?

E-Safety: Understanding the Risks

In addition to the 4 Cs the College uses a filtering system to protect users from inappropriate materials. Furthermore, the College monitors and logs use of the network, including the internet, and personal file space. All abuse or misuse is taken seriously and dealt with appropriately.

The College advises parents/carers to be aware of how, when and where their children are using technology. For example, apps they are using, websites they are visiting and games they are playing and adverts they are exposed to.

As parents/carers there may be occasions when you become aware of something that could place a staff member or student at risk. Depending upon the nature and timing of the matter there are several options open to you:

- Email the College safeguarding team, led by Mrs Matarazzo, using thinkpink@lvc.org;
- Telephone the College and ask to speak to one of the Safeguarding Team on 01223 891233;
- Telephone the NSPCC on 0808 800 5000 (24 hours a day, 365 days a year);
- If you feel the person is in immediate danger, don't delay, call the police on 999.

Some useful websites:

Internet Matters:
https://www.internetmatters.org/

UK Safer Internet Centre:
https://www.saferinternet.org.uk/

Child Exploitation and Online Protection command:
https://www.ceop.police.uk/safety-centre/

Think u Know:
https://www.thinkuknow.co.uk/

Childnet International:
http://www.childnet.com/

NSPCC:
https://www.nspcc.org.uk/

Use of Personal Technology – Student Agreement

Name: ________________________________ **Tutor Group: _________________**

Following assessments carried out by the Learning Support Department it has been agreed that I may use a laptop/tablet, henceforth referred to as a ‘device’. This must be used for tests and exams and in class when appropriate and practical. This will be considered my ‘normal way of working’.

This permission is granted and must be used according to the conditions below:

- The device is to be used in lessons for educational purposes only and its use will be directed by the teacher.
- The device should only be used to access the remote desktop, via http://access.lvc.org/. This will keep both myself and my work safe - my internet use will be filtered and monitored and my work will be backed up every evening. The exception to this is when specific software is only available on the device.
- Work must be provided for the teacher in the form requested and it is my responsibility to ensure the teacher receives it, whether this is by printing or emailing the work. This applies to all work, both in lessons and homework.
- I understand that the use of the device is also covered by the ‘Code of conduct for the use of technology’ and that ‘The college accepts no responsibility for any mobile technologies brought in and those who choose to bring them into college are responsible for them and bear the responsibility for any losses’ (see Student Handbook).
- I understand that where a school computer is available I will use this unless I need specific software that is only on my device.
- Inappropriate use of my device in lessons will be dealt with according to the school behaviour policy. Repeated misuse could lead to more serious consequences, such as loss of internet or removal of this opportunity.
- It is my responsibility to ensure that the device is fully functioning, including fully charged, and virus-free ready for use every day.

I have read the agreement, including the related policies, and agree to adhere to them.

Signed: ________________________________ **Date: _________________**

(Student)

I support the use of a laptop for my child and agree to the conditions outlined above.

Signed: ______________________________ Date: ________________

(Parent)

Information & Support

There is a wealth of information available to support Colleges and Colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

www.disrespectnobody.co.uk

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation