Policy No: 27.00

Policy and Procedure on

Online Safety

Cambian Dunbroch School

Policy Author / Reviewer	QI Team/Kate Brogan (IT Operations Manager)/Nicholas Foster (Data Protection Officer & Head of Information Governance
Approval Date	March 2025
Next Review Date	March 2026
Version No	4
Policy Level	Group
Staff Groups Affected	All Staff

Contents

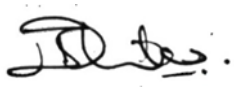
1. Monitoring and Review

1.1. The Proprietor will undertake a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one from the date of approval shown above, or earlier

if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

1.2. The Local content of this policy document will be kept under continuous monitoring and review by the Head of Service.

Signed:



Jeremy Wiles
Group Executive Director- Children's Services
August 2022

2. Terminology

2.1. Our aim is to use consistent terminology throughout this policy and all supporting documentation as follows:

'Establishment' or 'Location	this is a generic term which means the Children's School – Cambian Dunbroch School.
Individual	means any child or young person under the age of 18 or young adult between the ages of 18 and 25. At Cambian Dunbroch School we have Children and young people attending between the ages of 12 to 18
Service Head	This is the senior person with overall responsibility for the School. At Cambian Dunbroch School this is the Headteacher
Key Worker	Members of staff that have special responsibility for Individuals residing at or attending the Establishment.
Parent, Carer, Guardian	means parent or person with Parental Responsibility
Regulatory Authority	Regulatory Authority is the generic term used in this policy to describe the independent regulatory body responsible for inspecting and regulating services. At Cambian Dunbroch School, this is Ofsted
Social Worker	This means the worker allocated to the child/family. If there is no allocated worker, the Duty Social Worker or Team Manager is responsible.
Safeguarding Authority	Children's Social Care, Safeguarding Partners, Local Safeguarding Adults Board [LSAB] - England, Regional Safeguarding Children's Boards [RSCB] – Wales *whichever apply for the type of service and country
LADO	Local Authority Designated Officer
DSL/DSL Deputy	Designated Safeguarding Lead/Designated Safeguarding Lead Deputy
Placing Authority	Placing Authority means the local authority/agency responsible for placing the child or commissioning the service
Staff	Means full or part-time employees of Cambian, agency workers, bank workers, contract workers and volunteers.

3. Purpose

3.1. In all our Cambian services children, young people and young adults all have opportunities to interact with different technologies and in a wide range of situations. The exchange of ideas, social interaction and learning opportunities are greatly beneficial to all, but can occasionally place Individuals in danger. Cambian recognises this and wishes to guard against misuse as far as is possible as part of our duty of care.

3.2. The purpose of this policy and procedures is to:

3.2.1. To ensure that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

3.2.2. To create a balance between controlling access to the internet and technology, setting rules and boundaries and educating students/adults and staff/volunteers about responsible use.

3.2.3. To empower and educate the Individuals in our care so that they have the ability to make safe and responsible decisions and to report any concerns.

3.2.4. To ensure that all staff are aware of good e-safety practice so that they are able to educate and protect all Individuals in their locations.

3.2.5. To ensure that staff know how to manage their own professional reputation online and demonstrate appropriate online behaviours and the consequences of non-compliance.

4. Background

4.1. New technologies have become integral to the lives of Individuals/in today's society, both within Locations and in their lives outside of this. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps staff and Individuals learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

4.2. Individuals should have an entitlement to safe internet access at all times.

4.3. There is an Online safety section in 25.00 Child Protection and Safeguarding policy which addresses the training requirements, opportunity to teach safeguarding for both: staff and Individuals, remote learning, having broad and

balanced curriculum (schools and colleges) and helpful resources for schools and colleges in line with KCSIE2022. The policy also includes helpful hyperlinks for the schools about teaching online safety in schools.

4.4. The requirement to ensure that Individuals are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in Cambian locations are bound. This Online safety policy should help to ensure safe and appropriate use.

4.5. Cambian undertakes that development and implementation of such a strategy should involve all the stakeholders in an Individual's care and education from all members of care, education and clinical staff, parents, members of the community and the Individuals themselves.

4.6. The use of new technologies can put young people at risk. Some of the dangers they may face include:

4.6.1. Access to illegal, harmful or inappropriate images or other content

4.6.2. Unauthorised access to / loss of / sharing of personal information

4.6.3. Be subject to radical or extremist views

4.6.4. The risk of being subject to grooming by those with whom they make contact on the internet.

4.6.5. The sharing / distribution of personal images or videos without an individual's consent or knowledge

4.6.6. Inappropriate communication / contact with others, including stranger

4.6.7. Cyberbullying

4.6.8. Access to unsuitable video

4.6.9. An inability to evaluate the quality, accuracy and relevance of information on the internet

4.6.10. Plagiarism and copyright infringement

4.6.11. Illegal downloading of music or video files

4.6.12. The potential for excessive use which may impact on the social and emotional development and learning of the Individual

4.6.13. Risk of radicalisation (see also Preventing Extremism and Radicalisation Policy)

4.7. Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other Cambian policies (e.g. behaviour, anti-bullying and child protection and safeguarding policy).

4.8. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential where appropriate to build an Individual's resilience to the risks. It is also essential that where there is a possibility that an individual lacks mental capacity to make effective decisions around e-safety, that capacity assessments (MCA1 / MCA2) and if necessary Best Interest meetings are held to provide the correct level of support and or restrictions for those individuals when using technology.

Regulation off-site

4.9. **School** - The Education and Inspections Act 2006 empowers Headteachers/Principals in our Cambian Schools/Colleges, to such extent as is reasonable, to regulate the behaviour of Individuals when they are off the school/college site and empowers 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 out of school/college, but is linked to membership of the school/college.

4.10. **Children's Home**s/care homes for young people in children's services - This policy also covers the behaviour of Individuals when away from their home and under the care of staff. Each Individual's behaviour support plan and Risk

assessments need to take into consideration e-safety issues when supporting individuals in off-site areas, especially those which have access to the internet such as Internet cafes or business services' free WiFi.

4.11. Cambian will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/ carers of incidents of inappropriate e-safety behaviour that take away from the location whether this is the individual's home or education setting.

5. Roles and Responsibilities

5.1. The Information Governance Board for CareTech Holdings Plc is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

5.2. Within each Location we have the DSL who is the E –safety Lead for their service. The role of the DSL and DSL Deputy has been described in detail in 25.00 Child Protection and safeguarding policy and procedure/section 6: Roles and Responsibilities. The role includes taking the lead responsibility for referring and managing safeguarding and child protection issues/cases (including online safety), unless management of a particular case is passed on to a more senior member of the organisation.

5.3. Governance Boards in our schools and colleges and Regional Heads of Homes meetings will discuss e-safety incidents and monitoring reports.

The role of the Designated Safeguarding Lead (incorporating online safety)

5.4. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).

5.5. The Online Safety Lead (DSL) will take responsibility for ensuring that the following take place, in larger locations they may choose to elect an online safety Lead who will report directly to the DSL on issues of online safety:

- regular meetings with the online safety Lead (if applicable)
- regular monitoring of the online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governance Board meetings and Heads of Homes meetings
- Education – access Safeguarding Network home page for online safety resources and learning materials available

5.6. The Online Safety Lead should be trained in online safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise 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
- potential risk of radicalisation online

5.7. The Online Safety Lead should have and raise awareness amongst others of the following definition: "Online abuse is abuse that is facilitated using technology. It may take place through social media, online games, or other channels of digital communication. Children can also be re-victimised if evidence of their abuse is recorded or uploaded online. Technology can facilitate a number of illegal abusive behaviours including, but not limited to: harassment; stalking; threatening behaviour; sharing indecent images of children under 18; inciting a child to sexual activity; sexual

exploitation; grooming; sexual communication with a child; and, causing a child to view images or watch videos of a sexual act. Using technology to facilitate any of the above activities is online abuse."

Head of Service

5.8. Is responsible for ensuring the safety (including online safety) of all Individuals and staff.

5.9. Is responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

5.10. Will ensure that there is a system in place to allow for monitoring and support of those in school/college/homes who carry out the internal safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

5.11. Reports regularly to the school/college Governance board as well as the nominated Operations/Managing Director.

The Senior Leadership teams

5.12. Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the Location's online safety policies/documents.

5.13. Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

5.14. Provides training and advice for staff.

5.15. Accesses DfE advice for schools: teaching online safety in schools and shares helpful information with others.

5.16. Where required, liaises with the Local Authority.

5.17. Liaises with IT Department and its staff.

5.18. Reviews Online safety incidents and creates a log of incidents to inform and improve future online safety practice.

5.19. Will use external agencies such as JISC (post 16 provision) and the UK Council for Child Internet Safety to ensure that they are up to date with the current guidance.

5.20. Are aware of the Information and support available to schools and colleges to keep children safe online can be found in Part 2 and Annex B of2022.

5.21. IT Director/Technical staff - the Network Manager and ICT Co-ordinator are responsible for ensuring:

5.22. That Cambian's ICT infrastructure is secure and is not open to misuse or malicious attack.

5.23. That Cambian's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

5.24. That he/she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

5.25. That the use of the network/Virtual Learning Environment (VLE/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Designated Safeguarding Lead.

5.26. That monitoring software/systems are implemented and updated as agreed in Cambian policies.

Staff are responsible for ensuring that:

5.27. They have an up to date awareness of online safety matters including the definition of the online abuse which may be part of peer on peer abuse including sexual violence and sexual harassment (explored in 25.00 Child Protection and Safeguarding policy) and of the current online safety policy and procedures.

5.28. They have read and understood the GIG07 Information Systems Acceptable Use Policy.

5.29. They report any suspected misuse or problem to the Online Safety Lead for investigation/action/sanction.

5.30. Digital communications with students / pupils (email / Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using official Location systems.

5.31. Online safety issues are embedded in all aspects of the curriculum and other school/college activities, as applicable.

5.32. Individuals understand and follow the relevant online safety and GIG07 Information Systems Acceptable Use policy.

5.33. They monitor ICT activity in lessons and extra-curricular activities.

5.34. They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current policies with regard to these devices.

5.35. In class/ education settings where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

5.36. In the home where internet is used by Individuals that policy and procedures are followed and the level of support/monitoring balances the need for supporting Individuals to make appropriate choices for internet use with safeguarding them against risk of the various forms of internet abuse.

5.37. They never allow anyone else to log onto and use their account.

Individuals:

5.38. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

5.39. Should understand the importance of adopting good online safety practice when using digital technologies away from the Cambian Location and realise that Cambian Online Safety Policy covers their actions out of school/college, if related to their membership of the school.

Parents/Carers

5.40. Parents/Carers play a crucial role in ensuring that their children/ young person understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. Cambian locations will therefore take every

opportunity to help parents understand these issues through channels such as; parents' evenings, newsletters, letters, website/VLE and information about national/local e- safety campaigns/literature.

Teaching and Learning

5.41. At Cambian, the internet provides Individuals and staff with:

- access to worldwide educational resources including museums and art galleries; educational, social and leisure use
- access to experts in many fields for young people/adults and staff/volunteers;
- professional development for staff through access to national developments, educational materials and effective curriculum practice; collaboration across networks of schools, support services and professional associations
- exchange of curriculum and administration data with DfE; access to learning wherever and whenever convenient
- an opportunity to enhance and extend education
- ongoing contact with family members.

5.42. Young people/adults will be:

- given clear objectives when asked to use the internet.
- taught what internet use is acceptable and what is not.
- taught how to use the internet using age appropriate tools, and to use them effectively.
- taught how to evaluate materials sourced from the internet and to acknowledge those sources

5.43. Cambian will

- comply with copyright laws in line with the Copyright policy for the CareTech Group.
- provide access levels appropriate to the age and ability of the young person/adult
- ensure virus protection will be installed and updated
- have system security in place.
- Ensure adequate password management in place for Individuals and staff. (see Prevent Policy – Checklist Implications for IT)

6. Use of Email

6.1. Email is an essential means of communication for staff and enables communication between Cambian locations and other providers or interested parties locally and further abroad. Email can bring significant educational benefits.

6.2. It is important that staff understand they should be using a work provided email account only to communicate with parents/carers, young people/adults and other professionals for any official Cambian business. This is Important for confidentiality and security and also to safeguard members of staff from allegations.

7. Cambian Website

7.1. The contact details for each Cambian location on the website will be restricted to Cambian address, email and telephone number.

7.2. Staff or Individual's personal information will not be published.

7.3. The Group Business Development Director has overall editorial responsibility for online content published by Cambian. However, each Head of Service will have responsibility for ensuring that content published is accurate and appropriate.

7.4. The Cambian website will comply with Cambian's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

7.5. Heads of Service will continue to maintain an up-to-date list of photographic permissions for each individual and will ensure that no photographs are uploaded without appropriate permission.

8. Internet Use

8.1. All staff and volunteers at Cambian will sign and comply with Cambian's policies on use of the internet and mobile phones. They will be made aware that their online conduct could have an impact on their role and reputation within Cambian and further afield. Staff must read GHR 37 Code of Conduct and Teams Etiquette Guide (where Teams is being used).

8.2. Any member of staff finding access to a website containing inappropriate content will report it immediately to the ICT Department.

8.3. Parents/carers will be informed that Individuals will be provided with supervised internet access according to their age, ability and support needs.

8.4. Every Individual has an individual online safety risk assessment.

8.5. Some Individuals are unable to access technology and the internet independently, and for these the risk assessment states this. However, this will be reviewed regularly in line with care and educational planning.

8.6. For those who can access the technology and the internet independently, the risk assessment states the mitigating factors:

- (Name) is able to access the Internet independently
- There is always an adult in the room when (name) is on the Internet
- (Name) learns about online safety as part of ICT
- Adult and malicious sites are locked down on the network

8.7. Cambian will make specific decisions based upon the needs and levels of understanding of all Individuals at each Cambian location.

8.8. The senior management team should note that technologies such as mobile phones with wireless Internet access can bypass Cambian filtering systems and present a new route to undesirable material and communications.

9. Social Networks

9.1. Cambian recognises that the internet and digital media has numerous social networks that allow individuals to connect with people with similar and different interests. These also allow people to publish unmediated content. Examples of

social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chat rooms and instant messenger.

9.2. **Cambian teaching** staff will

- facilitate lessons or one-to-one sessions covering social networking for Individuals as and when relevant. The content of these lessons will include:
  - information about the most frequently used social networking sites, e.g. Facebook, Twitter, Skype, Instagram, snapchat, moshi monster, club penguin, Kik and Omegle.
  - information about the ease of uploading personal information, the associated dangers and the difficulty of removing inappropriate images and information once it has been published.
  - advice on sharing personal details, including friends and family personal security and privacy online.

9.3. Before any educational session starts, staff working with young people will assess the appropriateness of a site and the content to be accessed for safety.

9.4. **Cambian Care Staff** will:

- Ensure they have read and understood this policy and therefore support Individuals in a consistent manner
- Support Individuals to take full advantage of the internet, digital media and social networks within the guidelines of this policy.

9.5. **All Cambian Staff** will:

- Raise concerns with their line manager and if necessary the DSL, regarding the inappropriate use of social networking, social media and personal publishing sites (in and out of school/college), by young people, and will have regard for confidentiality. Parents/carers will be contacted by a senior member of staff if appropriate.
- Raise concerns according to the Whistleblowing Policy, regarding the inappropriate use of social networking, social media and personal publishing sites (in and out of Cambian), by staff. All parties will have regard for confidentiality.

10. Mobile Phones

10.1. Cambian has a policy on The Individuals' Use of Mobile Phones.

10.2. In education settings mobile phones will not be used during lessons or formal school time, unless as part of a lesson, where directed by a member of staff.

10.3. The sending of abusive or inappropriate text messages is forbidden.

11. Sexting - consensual and non-consensual sharing of nudes/semi-nudes images or/and videos

11.1. Sexting is also referred to as consensual and non-consensual sharing of nudes and semi-nudes images and/or videos (also known as sexting or youth produced sexual imagery). For more information about this read UKCIS guidance: Sharing nudes and semi-nudes advice for education settings.

11.2. This takes place when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages.

11.3. They can be sent using mobiles, tablets, smartphones, laptops - any device that allows you to share media and messages.

11.4. Sexting may also be called:

- trading nudes
- dirties
- pic for pic.

What the law says about sexting

11.5. Sexting can be seen as harmless, but creating or sharing explicit images of a child is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- take an explicit photo or video of themselves or a friend
- share an explicit image or video of a child, even if it's shared between children of the same age
- possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.

11.6. However, as of January 2016 in England and Wales, if a young person is found creating or sharing images, the police can choose to record that a crime has been committed but that taking formal action isn't in the public interest.

11.7. Crimes recorded this way are unlikely to appear on future records or checks, unless the young person has been involved in other similar activities which may indicate that they're a risk.

11.8. There are many reasons why a young person may want to send a naked or semi-naked picture, video or message to someone else.

- joining in because they think that 'everyone is doing it'
- boosting their self-esteem
- flirting with others and testing their sexual identity
- exploring their sexual feelings
- to get attention and connect with new people on social media
- they may find it difficult to say no if somebody asks them for an explicit image, especially if the person asking is persistent

What are the risks of sexting?

11.9. No control of images and how they're shared

- It's easy to send a photo or message but the sender has no control about how it's passed on.
- When images are stored or shared online they become public. Some people may think that images and videos only last a few seconds on social media and then they're deleted, but they can still be saved or copied by others.
- This means that photos or videos which a young person may have shared privately could still be end up being shared between adults they don't know.

11.10. Blackmail, bullying and harm

11.11. Young people may think 'sexting' is harmless but it can leave them vulnerable to:

- **Blackmail** - An offender may threaten to share the pictures with the child's family and friends unless the child sends money or more images.
- **Bullying** - If images are shared with their peers or in school, the child may be bullied.
- **Unwanted attention** - Images posted online can attract the attention of sex offenders, who know how to search for, collect and modify images.
- **Emotional distress** - Children can feel embarrassed and humiliated. If they're very distressed this could lead to suicide or self-harm.

How to deal with a disclosure of Sexting

11.12. If a young person tells you they've been involved with sexting, it's important to remain calm and be understanding.

11.13. Try and find out:

- if it's an image, video or message
- how the young person is feeling

- how widely has the image been shared and with whom
- if there were any adults involved
- if it's on an organisational or personal device

11.14. Follow the policy and procedure for raising concerns through the Child Protection-Safeguarding Policy - complete a concern form and hand this to the DSL within ONE hour.

11.15. The National Police Chief's Council (NPCC) recommends that safeguarding should be the main concern of any investigation into a sexting incident; and that we should avoid criminalising young people necessarily.

11.16. If the images were not intended to cause harm and the young people involved have given consent, you may decide to handle the incident within your organisation.

11.17. Avoid looking at the image, video or message. If it's on a device belonging to your organisation, you need to isolate it so that nobody else can see it. This may involve blocking the network to all users.

11.18. Details of the incident and the actions taken must be recorded in writing by the person responsible for child protection within the organisation.

11.19. Contact the police and children's social care if:

- somebody involved is over the age of 18 or under the age of 13
- there are concerns about the ability to give consent
- the images are extreme or show violence
- the incident is intended to cause physical or emotional harm
- there's reason to believe that the young person has been blackmailed, coerced or groomed

11.20. If you think a child is in immediate danger - call the police on 999 or call us on 0808 800 5000, straight away.

12. Use of Digital Images and Videos

12.1. The development of digital imaging technologies has created significant benefits to learning, and feeding back to parents/carers, allowing staff and Individuals instant use of images that they have recorded themselves or downloaded from the internet. However, staff and Individuals need to be aware of the risks associated with sharing images and with

posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

12.2. When using digital images, staff should inform and educate Individuals 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.

12.3. Staff are allowed to take digital/video images to support educational aims, but must follow Cambian's policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Cambian equipment; the personal equipment of staff should not be used for such purposes.

12.4. Care should be taken when taking digital/video images that Individuals are appropriately dressed and are not participating in activities that might bring the individuals or Cambian into disrepute.

12.5. Photographs published on the website, or elsewhere that include Individuals are carefully selected and comply with good practice guidance on the use of such images.

12.6. Individuals' full names will not be used anywhere on a website or blog, particularly in association with photographs.

13. Cyber-bullying

13.1. Staff should refer to Cambian's Anti-bullying Policy and Child Protection and Safeguarding policy.

13.2. Cyber-Bullying "Cyber-bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself." We recognise that the advent of cyber-bullying adds a new and worrying dimension to the problem of bullying as there no safe haven for the person being bullied. Unlike other forms of bullying, cyber-bullying can follow children and young people into their private spaces and outside school/college hours. Cyber-bullies can communicate their messages to a wide audience with remarkable speed, and can often remain unidentifiable and unseen. ICT may be used to send threatening pictures or messages to others.

13.3. Seven categories of cyber-bullying have been identified:

- Text message bullying involves sending unwelcome texts that are threatening or cause discomfort;
- Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- Online grooming, Chat room and Social Networking Site abuse involves sending menacing or upsetting responses to children or young people.
- Bullying through instant messaging (IM) is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online;
- Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

13.4. Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips have sent by mobile phone. Most cyber-bullying is done by children in the same class or year group. Although it leaves no visible scars, cyber-bullying of all types can be extremely destructive. We will offer

parents' information sessions on the dangers of cyber-bullying and on-line child protection issues at regular intervals. Research has found that:

- Between a fifth and a quarter of children have been cyber-bullied at least once over the previous few months;
- Phone calls, text messages and email are the most common forms of cyber-bullying;
- There is more cyber-bullying outside school than in;
- Girls are more likely than boys to be involved in cyber-bullying in school, usually by phone;
- For boys, text messaging is the most usual form of cyber-bullying, followed by picture/video clip or website bullying;
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyber-bullying;
- Website and text bullying are equated in impact to other forms of bullying;
- Around a third of those being cyber-bullied tell no one about the bullying.

14. Emerging Technology

14.1. Cambian will evaluate emerging technology for suitability before it is used in any Cambian location.

15. Management of Information Systems

15.1. Information Systems will be managed and maintained in line with the Information Security policy, including the following:

- The security of Cambian's systems and users will be reviewed regularly.
- Virus protection for the whole network and for individual machines (e.g. staff laptops), will be updated daily.
- Filtering systems will be in place to protect all at Cambian.
- Unsuitable sites will be blocked immediately once identified.
- Cambian will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to Cambian's network.
- All software will be installed by IT technicians so that checks can be made on the software for suitability, compatibility, etc., prior to installation.
- Files on Cambian's network will be checked regularly for content and malware.
- Concerns/issues and actions taken will be reported immediately to the ICT Manager so that s/he is fully informed.
- Servers will be located securely and physical access restricted.
- The server operating system will be secured and kept up to date.
- Access by wireless devices will be proactively managed and secured
- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Users must not share their log-in or passwords with anyone in or out of Cambian
- Laptops issued to staff must only be used by the allocated staff member.

16. Availability

16.1. The Online safety Policy will be formally provided and/or presented to and discussed with all members of staff and volunteers. Staff/volunteers will be informed that internet traffic can be monitored and traced to the individual user.

Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally will be provided for all members of staff.

16.2. Staff/volunteers should understand that phone or online communications with students/adults can occasionally lead to misunderstandings or even malicious accusations. Staff/volunteers must take care always to maintain a professional relationship. Staff/volunteers are asked not to have students/adults as 'friends' on social networking sites.

16.3. CAMBIAN will draw parents/guardian's attention to the Online safety Policy, provide basic information on internet safety as required, and links to child-friendly resources.

17. Standard Forms, Letters and Documents

This policy

17.1. None

Related Policy

17.2. 25 POLICY - Child Protection and Safeguarding

17.3. 26 POLICY - Safeguarding Prevent – Checklist for managing passwords

17.4. 13 POLICY - Mental Capacity and Consent

17.5. 21 POLICY - Anti-bullying

17.6. 40 POLICY - Individual's Use of Telephone, Mobile Phones and Information Technology

17.7. 45 POLICY - Behaviour Support

17.8. GIG 02 POLICY - Data Protection

17.9. GIG 04 POLICY - Information Security

17.10. GIG 07POLICY – Information Systems Acceptable Use Policy (AUP)

17.11. GIG 08 POLICY - Access to Records

17.12. GIG 09 POLICY - Confidentiality Code of Practice

Guidance

17.13. JISC

17.14. UK Council for Child Internet Safety

17.15. Sexting Advice for Professionals

17.16. www.bbc.co.uk/webwise

17.17. https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/

17.18. www.kidsmart.org.uk

17.19. www.thinkuknow.co.uk

17.20. www.bizzikid.co.uk

17.21. teaching online safety in schools;

17.22. Sharing nudes and semi-nudes: advice for education settings working with children and young people;

17.23. 'Undressed'

17.24. Online safety in schools and colleges: Questions from the governing board.

17.25. 360 safe website.

17.26. Harmful online challenges and online hoaxes