CORNWALL EDUCATION
LEARNING TRUST

Online Safety Policy

"Safeguarding is everyone's responsibility"

At Cornwall Education Learning Trust (CELT) we are committed to safeguarding and promoting the welfare of children and we expect all Trustees, Governors, staff and volunteers to share this commitment.

Adopted by (body): CELT Trustees
Approved date: October 2021
Review date: October 2022

This policy is part of the following suite of annually updated safeguarding policies:

1. Child Protection and Safeguarding
2. Supporting Children and School with Medical needs/ Managing Medicines
3. Mental Health and Wellbeing
4. **Online Safety**
5. Peer on Peer Abuse
6. Attendance
7. Staff Code of Conduct
8. Whistleblowing

Contents

Aims/Purpose: 3

Policy principles 3

Operational 3

Reviewing and evaluating online safety and ensuring good practice 4

Key features of effective practice: 4

Online Safety Policy Scope 5

Who does online safety affect, who is responsible for online safety and what are their roles? 5

How will the school provide online safety education? 9

Working with parents 10

Staff – INSET and training 10

Trustees and Governors 11

Online safety and the Law: 11

Useful links to external organisations 11

Appendices 14

Aims/Purpose:

To give all staff clear guidance to secure a safe and informed environment where IT and the internet are used responsibly to promote and enhance pupils' learning. This policy is designed to promote safe and responsible conduct from all users across CELT.

Policy principles

- The Trust *Online Safety Policy* aims to create an environment where pupils, staff, parents, Trustees, Governors and the wider school community work together to inform each other of ways to use the Internet responsibly, safely and positively.
- Internet technology helps pupils learn creatively, effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The *Online Safety Policy* encourages appropriate and safe conduct and behaviour when achieving this.
- Pupils, staff and all other users of school-related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.
- These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace.
- The policy is not designed to be a blacklist of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge, leading to a safer internet usage and year-on-year improvement and measurable impact on online safety. It is intended that the positive effects of the policy will be seen online and offline, in school and at home, and ultimately beyond school and into the workplace.

- *Keeping Children Safe in Education* (2021) categorises the issues into four areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;
    - **Contact:** being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes harm; for example, making, sending and receiving explicit images, or online bullying.
    - **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Operational

Each CELT school has a Designated Lead member of staff for online safety, with additional nominated staff members as appropriate. There is also a Designated Governor Lead. At each school, and on the associated website, the following information will be displayed:

Key Personnel

The Designated Safeguarding Lead (DSL) is: Mrs Emma Williams
Contact details: email: head@luxulyansch.org Telephone: 01726 850397

The Deputy DSL(s) is: Mr Stewart Gynn
Contact details: email: sgynn@mevagisseysch.org Telephone: 01726 850397

The Online safety Co-ordinator(s) is: Mr Stewart Gynn
Contact details: email: sgynn@mevagisseysch.org Telephone: 01726 850397

The nominated Safeguarding Governor is: Mrs Annie Butler
Contact details: email: AButler@gov.celtrust.org

The Executive Headteacher is: Mr Stewart Gynn
Contact details: email: sgynn@mevagisseysch.org Telephone: 01726 850397

The Chair of Governors is: Mrs Sandra Beardsmore
Contact details: email: SBeardsmore@gov.celtrust.org

Reviewing and evaluating online safety and ensuring good practice

Key features of effective practice:

- All staff understand online safety issues.
- Online safety is a school priority.
- Trustees, Governors, leaders and staff understand the importance of online safety and recognise the potential impact of online activity on children's mental health.
- Training in online safety is audited and provided to all staff. Members of staff within CELT have received accredited online safety training.
- Clear and transparent procedures exist for monitoring, logging, reporting incidents, evaluating, improving and measuring the impact of online safety practices. All staff, parents, pupils, Trustees and Governors know how to report an online safety incident as a safeguarding concern.
- The school uses recognised and accredited CELT providers for Internet provision and filtering.
- The *Online Safety Policy* is closely integrated with relevant policies and procedures relating to child protection, safeguarding, acceptable use, anti-bullying, anti-radicalisation and behaviour.
- The acceptable use policy agreements have been developed with, signed by, and agreed to by all users of school IT systems – pupils, parents, staff, Trustees, Governors, visitors and external contractors.
- The school promotes a real-world, responsible and positive outlook towards Digital Literacy and Citizenship and online safety aimed at preparing pupils for expected standards of behaviour in adult life and the workplace.

- The school relies on Government, DfE, National College for Teaching & Leadership and ICO guidance and documentation with regard to Data Protection, data storage and privacy compliance.

Online Safety Policy Scope

- The school *Online Safety Policy* and agreements apply to all pupils, staff, support staff and members of the wider school community who use, have access to or maintain school and school-related internet, computer systems and mobile technologies internally and externally.
- The school will make reasonable use of relevant legislation and guidelines to effect positive behaviour regarding ICT and Internet usage both on and off the school site. This will include imposing rewards and sanctions for behaviour and sanctions for inappropriate behaviour around Online safety – as defined as regulation of student behaviour under the Education and Inspections Act 2006.
- 'In Loco Parentis' provision under the Children Act 1989 also allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

The *Online Safety Policy* covers the use of:

- School-based ICT systems and equipment.
- School-based intranet and networking.
- School-related external internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites.
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing.
- School ICT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets.
- Pupil and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or internet facilities.
- Tablets, mobile phones, devices and laptops when used on the school site.

Who does online safety affect, who is responsible for online safety and what are their roles?

Senior Leaders and online safety lead:

- CELT is responsible for determining, evaluating and reviewing online safety policies to encompass teaching and learning.
- Each CELT school will monitor the use of its IT equipment and facilities by pupils, staff and visitors, and agreed criteria for acceptable use by pupils, school staff and Governors of internet

capable equipment for school-related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

- The *Online Safety Policy* is a result of a continuous cycle of evaluation and review based on new initiatives, and partnership discussion with outside organisations; technological and Internet developments, current government guidance and school-related online safety incidents.
- The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine INSET provision for staff and Governors and guidance provided to parents, pupils and local partnerships.
- Online safety provision is always designed to encourage positive behaviours and practical real-world strategies for all members of the school and wider school community.

The School Online Safety Coordinator:

- The school has a designated Online Safety Coordinator Mr Stewart Gynn who reports to the SLT and Governors and coordinates online safety provision across the school and wider school community. The Online Safety Coordinator liaises with SLT, the schools Designated Safeguarding Lead (DSL) and other senior managers as required.
- The school Online Safety Coordinator is responsible for online safety issues on a day-to-day basis and also liaises with Trust contacts and the CELT IT team.
- The school Online Safety Coordinator maintains a log of submitted online safety reports and incidents.
- The school Online Safety Coordinator audits and assesses INSET requirements for staff, support staff and Governor online safety training, and ensures that all staff are aware of their responsibilities and the school's online safety procedures. The coordinator is also the first port of call for staff requiring advice on online safety matters.
- Although all staff are responsible for upholding the school *Online Safety Policy* and safer internet practice, the Online Safety Coordinator, the DSL and SLT are responsible for monitoring internet usage by pupils and staff, and on school machines, such as laptops.
- The Online Safety Coordinator is responsible for promoting best practice in online safety within the wider school community, including providing and being a source of information for parents and partner stakeholders.
- The school Online Safety Coordinator (along with IT support) should be involved in any risk assessment of new technologies, services or software to analyse any potential risks.

Trustees' and Governors' responsibility for online safety:

- The Safeguarding Governor is responsible for online safety, and the school Online Safety Coordinator will liaise directly with the Governor with regard to reports on online safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community.

IT support staff and external contractors:

- CELT IT support staff and technicians are responsible for maintaining the school's networking, IT infrastructure and hardware. They are aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the internet is secure. The team ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
- External contractors, such as Classcharts, website designers/hosts/maintenance contractors should be made fully aware of and agree to the school's *Online Safety Policy*. Where contractors have access to sensitive school information and material covered by the GDPR, for example on school website or email provision.

Teaching and teaching support staff:

- Teaching and learning support staff need to ensure that they are aware of the current school *Online Safety Policy*, practices and associated procedures for reporting online safety incidents.
- Teaching and learning support staff will be provided with an online safety induction as part of the overall staff induction procedures.
- All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the acceptable use policies (See appendices) and code of conduct relevant to internet and computer use in school.
- All staff need to follow the school's social media guidance, in regard to external off-site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on Internet school messaging or communication platforms, for example email, VLE messages and forums and the school website.
- All teaching staff need to rigorously monitor pupil internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site.
- Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
- Be aware of online propaganda and help pupils with critical evaluation of online materials.
- Internet usage and suggested websites should be pre-vetted in lesson planning.
- If using their personal device in school, they comply with the school's acceptable user agreement.

Designated Safeguarding Lead (DSL):

- The DSL needs to be trained in specific online safety issues. Accredited training with reference to child protection issues online is advised – for example a CEOP accredited course.

- The DSL needs to be able to differentiate which online safety incidents are required to be reported to CEOP, local Police, LADO, Local Safeguarding Children's Board, Trust Safeguarding Lead, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.
- Possible scenarios might include:
    - Allegations against members of staff.
    - Computer crime – for example hacking of school systems.
    - Allegations or evidence of 'grooming'.
    - Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.
    - Producing and sharing of Youth Produced Sexual Imagery (YPSI).
- The DSL needs to ensure that online safety is promoted to parents and carers and the wider community.
- The DSL needs to maintain a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms. They need to also monitor the number of online safety incidents to identify gaps/trends and use this data to response to reflect need.
- Acting 'in loco parentis' and liaising with websites and social media platforms such as Twitter and Facebook to remove instances of illegal material or cyber bullying.

Pupils:

- Pupils need to be aware of how to report online safety incidents in school, and how to use external reporting facilities, such as the Click CEOP button or Childline number.
- Are required to use school Internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.
- Pupils need to be aware that school Acceptable Use Policies cover all computer, Internet and mobile technology usage in school, including the use of personal items such as phones.
- Pupils need to be aware that their Internet use out of school on social networking sites such as Instagram is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and pupils in terms of cyber bullying, reputation, YPSI or illegal activities.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Pupils need to take responsibility for keeping themselves and others safe online.
- Pupils need to take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies, assessing personal risk and behaving safely and responsibly to limit those risks.

Parents and Carers:

- Parents and carers are expected to support the school's stance on promoting good internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.
- All parents and carers are asked to discuss online safety issues with their children and reinforcing appropriate safe online behaviours at home.
- It is important that parents and carers role model safe and appropriate uses of technology and social media.
- All parents and carers are asked to identify changes in behaviour that could indicate that their child is at risk of harm online and seek help/support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- The school expects parents and guardians to sign the school's Acceptable Use Polices/Home School Agreement, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as extranets, websites, forums, social media, online reporting arrangement, questionnaires and the VLE.
- The school will provide opportunities to educate parents with regard to online safety.

Other users:

- External users with significant access to school systems including sensitive information or information held securely under the Data Protection Act should be DBS checked. This includes external contractors who might maintain the school domain name and web hosting – which would facilitate access to cloud file storage, website documents, and email.

How will the school provide online safety education?

Example curriculum opportunities:

- Online safety as a Computing teaching unit; how to judge the validity of website information (including propaganda on the Internet), how to remove cyber bullying, computer usage and the law, how to spot and remove viruses, why copyright is important.
- Online safety as a PSHE teaching unit: how to deal with cyber bullying, how to report cyber bullying, the social effects of spending too much time online, YPSI and knowing where to go for help.
- Online safety as part of pastoral care – form time activities, assemblies, year group presentations, tutorial opportunities.
- Online safety events – such as Safer Internet Day and Anti Bullying Week.

Particular behaviours which will be addressed might include:

- Explaining why harmful or abusive images on the Internet might be inappropriate or illegal.

- Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe.
- Explaining how accessing and / or sharing other people's personal information or photographs might be inappropriate or illegal.
- Youth Produced Sexual Imagery (YPSI) and online radicalisation.
- Teaching why certain behaviour on the Internet can post an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practices such as grooming can develop.
- Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.
- Teaching pupils to assess the quality of information retrieved from the Internet, including recognising how reliable, accurate and relevant information is – particularly information obtained from search engines.
- Informing pupils and staff of copyright and plagiarism infringement laws, and potential consequences with regard to copying material for homework and coursework, copying photographs and images on social networking sites, copying material for using in teaching materials, downloading music, video, applications or other software files illegally.
- Encouraging responsible and effective digital literacy skills which extend beyond school and into the workplace.
- The medical and social effects of spending too much time on the Internet, games consoles or computers.

Working with parents

Example information dissemination opportunities:

- Online safety information directly delivered to parents: letters, newsletters, website subscribed news emails, the school extranet, learning platform, software Apps, website, school social media sites or VLE.
- Parents Evenings, open days, transition evenings, or other events to take advantage of occasions when there are large numbers of parents in school.
- Twilight courses or a series of presentations run by the school for parents and wider school community stakeholders.

Staff – INSET and training

Example training and information dissemination opportunities:

- Online safety information directly delivered to staff: letters, newsletters, website subscribed news emails, the school extranet, learning platform, school social media sites, website or VLE.
- A planned calendar programme of online safety training opportunities to be made available for staff, including on site Inset, whole staff training, online training opportunities (for example

Online safety Support courses), external CPD courses, accredited CPD courses, (for example CEOP) and Coordinator training.

- The *Online Safety Policy* will be updated and evaluated by staff at the beginning of each academic year and timetabled into the INSET day schedule.
- The Online Safety Coordinator should be the first port of call for staff requiring online safety advice.

Trustees and Governors

Example training and information dissemination opportunities:

- Online safety information directly delivered to Governors: letters, newsletters, website subscribed news emails, the school extranet, learning platform, school social media sites or website .
- Open days, or other events to take advantage of occasions when there are large numbers of visitors in school.
- Twilight courses or a series of presentations run by the school for parents and wider school community stakeholders.
- Governors should also be provided access to staff inset training, or specific Governor training provided externally (for example Online safety Support course or by the LA, Trust or Alliance, NAACE online or the National Governors Association.)

Online safety and the Law:

Computer Misuse Act 1990, sections 1-3
Data Protection Act 1998
Freedom of Information Act 2000
Communications Act 2003 section 1,2
Protection from Harassment Act 1997
Regulation of Investigatory Powers Act 2000
Copyright, Designs and Patents Act 1988
Racial and Religious Hatred Act 2006
Protection of Children Act 1978
Sexual Offences Act 2003
The Education and Inspections Act 2006 (Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause disturbance in class/breach the school behaviour policy.)

Useful links to external organisations

Ofsted: www.gov.uk/government/publications/school-inspection-handbook

DfE: www.gov.uk/government/groups/uk-council-for-child-Internet-safety-ukccis

CEOP:

- www.ceop.police.uk/safety-centre/
- www.childnet.com/

UK Safer Internet Centre:

- www.saferInternet.org.uk/safer-Internet-day
- www.saferInternet.org.uk/

Links to training:

Online safety Support: online refresher training www.online safetysupport.com/online_training
CEOP: www.ceop.police.uk/training/

Movies and presentations:

www.swgfl.org.uk/Staying-Safe/online safety-Movies
www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware

Other publications:

- Safer children in a digital world: the report of the Byron Review (PP/D16(7578)/03/08), DCSF and DCMS, 2008; http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/byronreview/.
- Ofcom's response to the Byron Review, Ofcom, 2008; http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/byron/.

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk

    - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
    - ChildLine: www.childline.org.uk
    - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

Appendices

Protocol for Online Communication and Safer Use of Technology

Managing the school/setting website

- The Trust will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- Contact details on the website will consist of the school/setting address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- School websites will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- The Trust will ensure that each school will post information about safeguarding, including online safety, on the school website for members of the community.

Publishing images and videos online

- All images and videos shared online are used in accordance with the policy regarding images of pupils
- The use of images and videos is in accordance with other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.
- In line with the Image Policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

Managing email

- Pupils may only use school/setting-provided email accounts for educational purposes
- All CELT staff are provided with a specific school/setting email address to use for any official communication.
- The use of personal email addresses by staff for any official school/setting business is not permitted.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Members of the community must immediately tell a designated member of staff (CELT IT/DSL) if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

Appropriate and safe classroom use of the internet (and associated devices)

- Internet use is a key feature of educational access and all children will receive age- and ability-appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please see Curriculum Statement/policies for further information.
- Individual school/setting's internet access will be designed to enhance and extend education.
- The Trust will ensure that access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability:

  - At Early Years Foundation Stage and Key Stage 1, pupils' access to the Internet will be led by adult demonstration with occasionally directly supervised access to specific and approved online materials which support the learning outcomes planned for the pupils' age and ability.
  - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
  - Secondary, Sixth Form pupils will be appropriately supervised when using technology, according to their ability and understanding.

- All school owned devices will be used in accordance with the school's Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school/setting will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The school/setting will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
- The school will use the Internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

Social Media Policy

General social media use

Expectations regarding safe and responsible use of social media will apply to all members of CELT community and exist in order to safeguard both the school/setting and the wider community, on- and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- All members of CELT community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of CELT community.
- All members of CELT community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school/setting will control pupil and staff access to social media and social networking sites whilst on site and using school-provided devices and systems
- The use of social networking applications during school hours for personal use **is not** permitted,
- Inappropriate or excessive use of social media during school/work hours or whilst using school/setting devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of CELT community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as Anti-Bullying, Allegations Against Staff, Behaviour and Safeguarding/Child Protection.
- Any breaches of school/setting policy may result in criminal, disciplinary or civil action being taken, and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as Anti-Bullying, Behaviour, Staff Code of Conduct, Safeguarding and Child Protection including the 'Allegations Against Staff' section.

Official use of social media

- CELT official social media channel is via Twitter.
- Each school/setting has their own official social media channels, in line with CELT social media guidance.
- Official use of social media sites by the school/setting will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official school/setting social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Each school will use school/setting-provided email addresses to register for and manage any official approved social media channels.

- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including CELT social media guidance, Anti-Bullying and Child Protection and Safeguarding.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school/setting website and take place with written approval from the Leadership Team.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Public communications on behalf of the school/setting will, where possible, be read and agreed by at least one other colleague.
- The school/setting will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff personal use of social media

The following links may be helpful to share with members of staff:

(childnet.com) Teachers and Professionals - for you as a professional

(childnet.com) Teachers and Professionals Professional Reputation

(saferinternet.org.uk) Teachers and Professionals Professional Reputation

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of their staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school/setting Acceptable Use Policy and CELT Staff Code of Conduct
- All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the Designated Safeguarding Lead and/or a member of the Leadership Team/Headteacher.
- If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school-provided communication tools.

- All communication between staff and members of the school community on school business will take place via official approved communication channels
- Staff will not use personal accounts or information to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils/parents received on personal social media accounts will be reported to the Designated Safeguarding Lead.
- Information to which staff members have access as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with CELT schools' policies and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- Members of staff will ensure that they do not represent their personal views as that of the school/setting on social media.
- School/setting email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the school/settings social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the school/setting, then they are requested to be professional at all times and are reminded that they are an ambassador for the school/setting.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school/setting.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.

- Staff must ensure that any images posted on any official social media channel have appropriate written parental consent to do so.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school/setting unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the Headteacher/Leadership Team of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
- Staff using social media officially agree to the Acceptable Use Policy and sign the Staff Code of Conduct Policy annually.

Pupils' use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy and Home School agreements.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age-appropriate sites which have been risk-assessed and approved as suitable for educational purposes.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on the appropriate security on social media sites and will be encouraged to use it safely and with passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school/setting where possible.
- The school/setting is aware that many popular social media sites state that they are not permitted for children under the age of 13, therefore the school will not create accounts within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school and CELT policies.

- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

Use of Personal Devices and Mobile Phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of CELT community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school/setting and is covered in appropriate policies including the CELT schools' Acceptable Use Policy.
- CELT recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools/settings.

Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school and CELT policies.
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school/setting accepts no responsibility for the loss, theft or damage of such items. Nor will the school/setting accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school/setting.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Discipline/Behaviour Policy.
- All members of CELT community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of CELT community will be advised to use passwords/PIN numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and PIN numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of CELT community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school/settings policies.
- School/setting mobile phones and devices must always be used in accordance with the Acceptable Use Policy and Staff Code of Conduct where appropriate.
- School/setting mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the Acceptable Use Policy.
- Pupils' personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during lessons and while moving between lessons.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If a pupil needs to contact their parents/carers they will be allowed to use a school/setting phone.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Headteacher.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school's policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Anti-bullying policy. The phone or device may be searched by a member of the Leadership Team with the consent of the pupil or parent/carer. Searches of mobile phone or personal devices will be carried out in accordance with the school policy on (gov.uk) Searching Screening and Confiscation. If there is a suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, then the device will be handed over to the police for further investigation.

Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.

- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school/setting policy, disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, then the police will be contacted.
- Any allegations against a member of staff involving personal use of mobile phone or devices will be responded to following the allegations management section in the school/setting's Safeguarding and Child Protection Policy.

Visitors' use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school/setting's Acceptable Use Policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must be in accordance with the school/setting's Image Use Policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use of personal devices.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead/Headteacher of any breaches of use by visitors.

Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content (see illegal incidents flowchart).
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
    - pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- CELT require staff, parents, carers and pupils to work in partnership to resolve online safety issues.

- After any investigations are completed, CELT will debrief, identify any lessons to be learned and implement any policy or curriculum changes as required.
- Safeguarding concerns and incidents should be reported to the MARU, in line with CELT Safeguarding and Child Protection policy.
- If they are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the MARU.
- Where there is suspicion that illegal activity has taken place, we will contact the CSPA or Surrey Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Head will speak with Surrey Police first to ensure that potential investigations are not compromised.

Concerns about Pupils' Welfare

- The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or deputies) will record these issues in line with the CELT Safeguarding and Child Protection Policy.
- The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the CELT Child Protection and Safeguarding policy.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our Staff Code of Conduct.

Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

- CELT schools and settings have accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2021) guidance and part 5 of 'Keeping children safe in education' 2021
- CELT recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised

online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within the CELT Peer on Peer Abuse policy.
- CELT recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- CELT also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- CELT will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on pupils electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with the School Behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Sexting")

- CELT recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- CELT schools/settings will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.

- CELT will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- CELT will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- CELT will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using setting provided or personal equipment.
- CELT will not:
  - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
    - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
  - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policies and the relevant CELT Safeguarding Child Board's procedures.
  - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
  - Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - Carry out a risk assessment which considers any vulnerability of pupils involved; including carrying out relevant checks with other agencies.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - Make a referral to Children's Social Care and/or the Police, as appropriate.
  - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
  - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
  - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- CELT will review the handling of any incidents to ensure that best practice was implemented; the school/setting Leadership Team will also review and update any management procedures, where necessary.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- CELT will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- CELT recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- CELT will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.
- CELT will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our Safeguarding and Child Protection Policies and the relevant Safeguarding Children Board's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Care (if required/appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- CELT will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting-provided or personal equipment.
    - Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
    - If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Standards and Learning Effectiveness Service and/or Police.
- If pupils at other school/settings are believed to have been targeted, the DSL (or deputy) will seek support from the Police and/or the Standards and Learning Effectiveness Service first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- CELT will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police and/or the Standards and Learning Effectiveness Service.
- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy and the relevant CELT Safeguarding Child Boards procedures.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Surrey police or the LADO.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
  - Ensure that the DSL (or deputy DSL) is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
  - Ensure that the DSL (or deputy DSL) is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
  - Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
  - Quarantine any devices until police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at CELT.

Online Hate

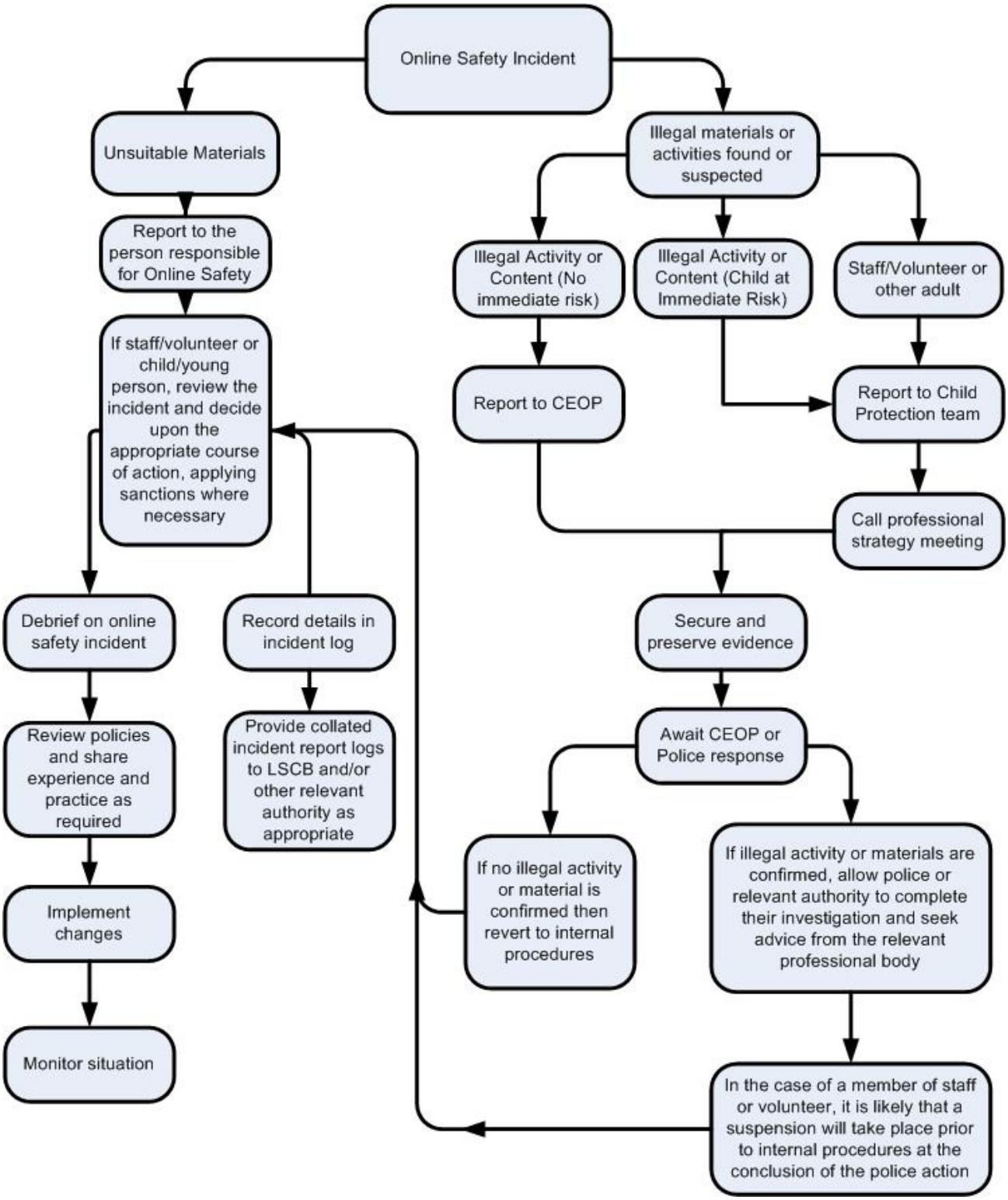
- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at CELT and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice through the Standards and Learning Effectiveness Service and/or Surrey Police.

Online Radicalisation and Extremism

- CELT will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the Internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our Child Protection Policy.
- If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher/Leadership Team will be informed immediately, and action will be taken in line with the appropriate Safeguarding policies.

Illegal incidents Flowchart

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 this Flowchart for responding to online 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