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.

This policy is part of the following suite of annually updated safeguarding policies:
Child Protection and Safeguarding
Supporting Children and School with Medical needs/ Managing Medicines
Mental Health and Wellbeing
Online Safety
Child on Child Abuse including Antibullying
Attendance
Staff Code of Conduct
Whistleblowing

Contents

Aims

- Robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective and positive approach to online safety, which empowers us to protect and educate the whole community in its use of technology
- Educate the whole school community about their access to and use of technology and
- Establish effective mechanisms to identify, intervene and escalate incidents where appropriate.
- Establish clear mechanisms to identify, intervene and escalate an incident where appropriate.
- Promote a culture of safety, equality and protection in school.

Policy principles

Cornwall Education Learning Trust (CELT) 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.
- recognise the significant impact of the global pandemic. Pupils have spent significantly more time online than would typically have been the case. Whilst some of this time has been positive and important for their educational and social needs, CELT recognises the increased level of risk that is now evidenced.
- recognise that many pupils have access to the internet via their mobile phone. CELT schools will manage access to phones carefully and ensure that the PSHE and Computing curricula, enable pupils to use technology responsibly and safely.
- promote the support available through National Online Safety and increase staff and pupil awareness of staying safe online.
- operate and monitor a safe online space in all CELT schools supported by Smoothwall filtering and monitoring software. This software connects the monitoring of online behaviours with CPOMS software to enable staff to manage and support staff and pupil's internet access on any school owned device.
- encourage pupils, staff and all other users of school-related technologies to work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.
- have acceptable use agreements to promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace (see appendices)
- not to have 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.

- have positive effects on all users when online and offline, in school and at home, and ultimately beyond school and into the workplace.

Keeping Children Safe in Education (2024) categorises the issues into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racism, misogyny, self-harm, anti-semitism, radicalization and extremism.;
- **Contact:** being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct:** personal online behaviour that increases the likelihood of, or causes harm; for example, making, sending and receiving explicit images, or online bullying and
- **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. At each school, and on the associated website, the following information will be displayed:

Key Personnel
The Online safety Lead is: Abby Macdonald Contact details: amacdonald@celtrust.org.uk The Designated Safeguarding Lead (DSL) is: XXX Contact details: dsl@XXX The nominated Safeguarding Governor is: XXX

Policy Scope
CELT's Online Safety Policy and agreements apply to all staff including governing bodies, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' as well as pupils/students and parents/carers

CELT 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. And will meet the school's responsibility under:

- Education Regulations 2014
- Statutory framework for the Early Years Foundation Stage
- Education and Skills Act
- Children Act
- Childcare Act
- Data Protection Act
- Equality Act.
- Keeping Children Safe in Education

The online safety policy is part of CELT Safeguarding suite of policies and should be read in conjunction with them as well as the school's behaviour policy.

CELT will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as technology). Examples of use include;

- school-based ICT systems and equipment
- school-based intranet and networking
- any Trust owned laptop or device loaned to pupils
- 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

Roles and Responsibilities
Trustees' and Governors':

- the Lead Trustee, on behalf of the Board, for Safeguarding is responsible for the Trust oversight of online safety
- the LGB safeguarding governor, on behalf of the LGB, is responsible for the school oversight of online safety, and the school online safety lead will liaise directly with the Governor with regards to reports on online safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community

The School Online Safety Lead:

- report to the SLT and Governors on a regular basis on online safety effectiveness, incidents, monitoring, evaluation
- liaises with SLT, the schools Designated Safeguarding Lead (DSL) and other senior managers as required
- oversees the log of submitted online safety reports and incidents
- 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 including understanding filtering and monitoring
- first port of call for staff requiring advice on online safety matters
- promoting best practice in online safety within the wider school community, including providing and being a source of information for parents and partner stakeholders
- ensure online safety is part of staff induction
- ensure staff, pupils and parents/carers are aware of this policy and related acceptable use policies

IT support staff and external contractors:

- maintaining the school's networking, IT infrastructure and hardware
- be aware of current thinking and trends in IT security and ensure that CELT's systems, particularly file-sharing and access to the internet is secure
- 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
- ensure there are risk assessments of new technologies, services or software to analyse any potential risks
- ensure adequate security policies are in place to patch and update system vulnerabilities and ensure technologies such as Multi Factor Authentication are enabled to limit the opportunity for external attack on cloud storage and email external contractors, such as Classcharts, website designers/hosts/maintenance contractors, where they have access to sensitive school information and material covered by the GDPR, for example on school website or email provision, should be made fully aware of and agree to the school's Online Safety Policy
- Provide support and training to staff in keeping files secure. In order to facilitate MFA staff will be expected to use the most cost effective solution available to the trust and as such it will be acceptable to make use of mobile phone / personal device technology within the classroom

Teaching and teaching support staff:

- aware of and understand the systems in place to support pupils online safety, how to manage them effectively and know how to escalate concerns to the Online safety lead when identified

- ensure that they are aware of the current school Online Safety Policy, practices and associated procedures for reporting online safety incidents
- ensure that they have read, understood and signed (thereby indicating an agreement) the acceptable use policy that includes social media, on site use, external off-site use, personal use and conduct on Internet school messaging or communication platforms, for example email, VLE messages and forums and the school website
- deliver online safety lessons throughout the curriculum
- 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
- when storing files and documents to use preferred and accepted storage as One Drive and SharePoint.
- promote best practice regarding avoiding copyright infringement and plagiarism
- be aware of online propaganda and help pupils with critical evaluation of online materials
- ensure internet usage and suggested websites are pre-vetted in lesson planning
- if using their personal device in school, they comply with the school's acceptable user agreement
- liaise with the safeguarding team if concerns arise around a pupils online use
- ensure staff understand what filtering and monitoring is and this is embedded and robust to prevent pupils accessing both inappropriate and harmful content online whilst in school or at home using school devices.
- ensure staff adhere to CELT security and compliance policies, such as making use of multi factor authenticator (MFA) to enhance security, regularly restarting devices to allow essential updates to take place, reporting suspect emails and attempts to breach CELT systems
- ensure staff do not sign up for systems or software, or online portals before relevant GDPR checks and DPIA's have been undertaken even when such systems are free of charge.

Designated Safeguarding Lead (DSL):

- access training to support vulnerable pupils
- be able to differentiate which online safety incidents are required to be reported to local Police, LADO, Trust Safeguarding Lead, children 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 nude or semi nude images
- ensure that online safety is promoted to parents and carers and the wider community
- take a lead role, in addition to the Online Safety Coordinator and members of the Senior Leadership team to understand and communicate the filtering and monitoring system in place at the school to all staff and parents/carers
- maintain a record of online safety concerns/incidents and actions taken on CPOMS
- monitor the number of online safety incidents to identify gaps/trends and use this data to response to reflect need and liaise with the online safety lead
- 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 (at a level that is appropriate to their individual age, ability and vulnerabilities):

- know how to report online safety incidents in school, and how to use external reporting facilities, such as contacting Childline
- engage in age-appropriate online safety education opportunities
- respect the feelings and rights of others both on and offline
- follow the school acceptable use policy. To sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf
- understand that school Acceptable Use Policies cover all computer, Internet and mobile technology usage in school, including the use of personal items such as phones on school site
- understand 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, nude or semi nude pictures 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:

- 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
- discuss online safety issues with their children and reinforcing appropriate safe online behaviours at home
- role model safe and appropriate uses of technology and social media
- 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
- 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

- Engage in opportunities provided by the school to understand how to support their children online

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

Teaching and Learning

Pupils are taught about safeguarding, including online safety, through teaching and learning opportunities within the curriculum. In addition, these messages are reinforced as part of assemblies, tutorial or pastoral activities.

Pupils are taught about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices. Those parts of the curriculum that deal with the safe use of technology are reviewed on a regular basis to ensure their relevance

Pupils are taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.

Pupils are taught about the risks associated with using the technology and how to protect themselves and their peers from potential risks.

Pupils are taught how to recognise suspicious, manipulative, dishonest, bullying or extremist behaviour.
Pupils are taught the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect.

Pupils are taught how to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat and how the school will deal with those who behave badly

Pupils are taught the consequences of negative online behaviour.

Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Pupils are helped to understand the need for the Acceptable Use appendices in this policy and encouraged to adopt safe and responsible use both within and outside school. Pupils are reminded of the importance of the Acceptable Use appendices in this policy on a regular basis.

In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in

internet searches.

Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the pupils visit. In such circumstances, staff will be mindful of the needs of those pupils, including providing additional support to pupils with SEND who may require additional support to stay safe online.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that IT Support temporarily remove specific websites from the filtered list for the period of study. Any request to do so should be raised via the IT Service Desk, with clear reasons for the need.

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
- nude and semi nude images 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

Filtering and Monitoring

CELT aim to limit children's exposure to the above risks from the school's IT system.

- the school will work in partnership with a chosen provider, Smoothwall, to ensure systems to protect pupils and staff are reviewed and improved

- all users are informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- strategies to ensure safe online behaviour and responsible use of new technologies for both staff and pupils is in place at all CELT schools through the use of continuous monitored filtering software
- if staff or pupils come across unsuitable on-line materials, the site must be reported to the service desk
- senior staff will ensure that regular reviews are made to ensure that the filtering methods selected are appropriate, effective and reasonable and that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding. The filters are set to age-appropriate filtering and monitoring sysems
    - Illegal content eg. child sexual abuse images is filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list.
    - The filtering system blocks sites that fall into categories such as pornography, racial hatred, extremism, self-harm, violence, drugs / substance abuse, hacking, piracy, gaming, and sites of an illegal nature.
    - Content lists are regularly updated and Internet use is logged and regularly monitored.
    - The filtering system provides appropriate filtering levels for different ages and groups of users such as staff, primary school pupils and secondary school pupils.
    - The filtering and monitoring systems are configured to send automated safeguarding alerts and reports to the safeguarding team to help identify pupils who are likely to be at risk based on their usage of IT in school.
- any inappropriate content should be reported to the IT helpdesk
- password integrity for filtering will be monitored by the IT helpdesk
- follow DfE's latest filtering and monitoring standards and cyber security standards for schools and colleges
- due to the global and connected nature of the Internet, it is not possible to guarantee that unsuitable or offensive material cannot be accessed via a school computer or device.
- all users must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity.
    - use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. Pupils must tell a member of staff immediately if they have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

- the Designated Safeguarding Lead runs half termly checks to ensure that the filtering systems are fit for purpose.

Staff training and development

CELT takes the training of its employees seriously. The online safety lead will regularly audit the need within the school and tailor the support accordingly.

As part of induction, all new staff will be provided with a copy of this policy. They will also be introduced to the online safety lead who will explain their role. Either a safeguarding team member or the online safety lead will provide them with basic online safety training so that they are aware of how to deal appropriately with incidents involving the use of technology when they occur. This includes being able to recognise the additional risk that children with SEN and disabilities (SEND) face online, so that staff are confident they have the capability to support SEND children to stay safe online.

Where safeguarding incidents involve youth produced sexual imagery, staff will follow the principles laid out in the CELT Child Protection policy, and Keeping Children Safe in Education

All staff members will be provided with online safety updates as part of their routine safeguarding and child protection training including on specific safeguarding issues such as sharing nudes and semi-nude images and or videos, cyberbullying, radicalisation, dealing with harmful online challenges and online hoaxes and cyberattacks.

All members of the school community will be made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the Acceptable Use appendices in this policy and highlighted through a variety of education and training approaches

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, including on site Inset, whole staff training, online training opportunities (for example Online safety Support courses) or external CPD courses
- the Online Safety Policy will be updated and evaluated by staff at the end of each academic year and timetabled into the INSET day schedule

Misuse of technology

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Security and Management of Information Systems

CELT takes appropriate steps to ensure the security of our information systems, including;

- virus protection being updated regularly
- encryption for personal data sent over the internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems
- not using portable media without specific permission;
- not downloading unapproved software to work devices or opening unfamiliar email attachments
- regularly checking files held on the school's network
- the appropriate use of user logins and passwords to access the school network
- all users are expected to log off or lock their screens/devices if systems are unattended and change passwords regularly
- all users are expected to make use of enhanced security technologies such as Multi Factor Authentication when logging into academy systems and to choose enhanced security options even if this is not the default option.

Use of Video Conferencing Technology

Online meeting invitation links must not be shared with or accessed by others unless permission has been granted by the meeting organiser.

The use of on-line learning tools and systems must be in line with privacy and data protection requirements

When delivering on-line lessons, the following must be adhered to.

- normally, no 1:1 activity with pupils, groups only. When 1:1 contact is required, such as for well-being calls, careers interviews or post-16 tutorials, these calls may be made by phone, in line with the Code of Conduct, or using Teams. Any 1:1 Teams calls must be recorded using the record function with the recording being retained by the teacher.
- staff must wear appropriate clothing, and anyone else in the household who may appear must be clothed.
- any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred or with a professional background.
- live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.

- language must be professional and appropriate, including any family members in the background.
- staff must only use platforms provided by the school to communicate with pupils.
- staff should record, the length, time, date and attendance of any sessions held.
- staff must follow Trust guidance when setting up on-line lessons to ensure that appropriate safeguarding settings are in place to prevent unauthorised use and access to on-line lessons

Digital Images and Videos
The school will gain parental/carer permission for use of digital photographs or video involving their child.

The school does not include the full names of pupils in online photographic materials or in the credits of any published school-produced video materials / DVDs.

Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that posting photos which in the reasonable opinion of the Headteacher could amount to a criminal offence, or which brings the school into disrepute, on any form of social media or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures in line with the behaviour policy.

Pupils are taught that they should not post images or videos of others without their permission. They are taught about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school.

Pupils are advised about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Sharing nudes and semi-nude images (sexting/youth produced sexual imagery):

- pupils are taught about the risks of sharing nudes and semi-nude images and how to report any concerns to a member of staff.

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
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
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
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

School Procedures

All pupils, members of staff and other adults have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that all users are fully aware of their responsibilities when using technology, they are required to read and sign the appropriate Acceptable Use appendix, where possible this is done electronically.

In the event of an online safety incident involving illegal activity, the school will follow the principles outlined in Safeguarding Suite of Policies.

Online safety incidents that involve inappropriate rather than illegal activity will be dealt with through the school's Behaviour, Child-on-Child Abuse including Anti-Bullying and Child Protection Policies, as appropriate.

Anyone who has any concern about the welfare and safety of a pupil must report it immediately to the DSL in accordance with the school's Child Protection Policy and procedures.

The school reserves the right to withdraw access to the school's network by any user at any time and to report suspected illegal activity to the police.

Where staff identify technical deficiencies, or opportunities to improve the school's filtering and monitoring systems they will report these via the IT Service Desk.

Monitoring and evaluation

The school recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The school will:

- regularly review the methods used to identify, assess and minimise on-line risks
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted

The school will review the filtering and monitoring provision and associated processes at least annually, or when there has been a significant implementation or change to the technology used at the school.

The LGB or RIG will appoint a safeguarding governor who will visit the school regularly and meet with the online safety lead. They will provide a report at each meeting using the CELT safeguarding visit template to support CELT in fulfilling its requirement to ensure that the school's arrangements for online safety are effective.

The CELT Trust Safeguarding Lead will, through the scheme of Quality Assurance offer assurances

to the Trustees that filtering and monitoring systems are effective across the Trust.

APPENDIX 1a - Acceptable use agreement (pupils and parents/carers) – EYFS + KS1

Acceptable use agreement (pupils and parents/carers)	
Name of pupil:	
These online safety rules help to protect pupils and the school by describing acceptable and unacceptable use of devices and systems (including computers, mobile devices and learning platforms).	
This is how we stay safe when we use computers: • I will ask a teacher or suitable adult if I want to use the computers/tablets • I will only use activities that a teacher or suitable adult has told or allowed me to use. • I will take care of computers/tablets and other equipment. • I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong. • I will keep my personal information and passwords safe online. • I will tell a teacher or suitable adult if I see something that upsets me or makes me feel worried on the screen. • I know that if I break the rules I might not be allowed to use a computer/tablet.	
Parent/Carer: • I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. • I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these. • I understand that my child will not be allowed to bring an electronic device, including mobile phones to school.	
Pupil signed:	**Date:**
Parent signed:	**Date:**

APPENDIX 1b - Acceptable use agreement (pupils and parents/carers) KS2

Acceptable use agreement (pupils and parents/carers)

Name of pupil:

These online safety rules help to protect students and the school by describing acceptable and unacceptable use of devices and systems (including computers, mobile devices and learning platforms).

I will read and follow the rules in the acceptable use agreement policy.

Safe

- **I only send messages which are polite and friendly.**
- **I will keep my privateinformation safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer**
- **I will only post pictures or videos on the internet if they are appropriate and if I have permission.**
- **I only talk with and open messages from people I know and I only click on links if I know they are safe.**
- **I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.**

Trust

- **I know that not everything or everyone online is honest or truthful and will check content on other sources like other websites, books or with a trusted adult.**
- **I always credit the person or source that created any work, image or text I use.**

Responsible

- **I always ask permission from an adult before using the internet.**
- **I only use websites and search engines that my teacher has chosen.**
- **I use school computers for school work, unless I have permission otherwise.**
- **I keep my personal information safe and private online.**
- **I will keep my passwords safe and not share them with anyone.**
- **I will not log on, access or change other people's files or information.**
- **I will only change the settings on the computer if a teacher/technician has allowed me to.**
- **I will always log off or shut down a computer when I've finished working on it.**

Understand

- **I understand that the school's internet filter is there to protect me, and I will not try to bypass it.**
- **I know that my use of school devices/computers and internet access will be monitored and if not used appropriately there will be consequences.**
- **I know that I can visit www.thinkuknow.co.uk, www.childnet.com and www.childline.org.uk to learn more about keeping safe online.**

Tell

- **If I am aware of anyone being unsafe with technology then I will report it to a teacher.**
- **I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.**
- **If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away.**

If I bring a personal mobile phone or other personal electronic device into school:

- I will hand my device in at the beginning of the day.

<table>
<tr><td colspan="2">

I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission
I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

</td></tr>
<tr><td colspan="2">
Parent/Carer:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.
I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

</td></tr>
<tr><td>Pupil signed:</td><td>Date:</td></tr>
<tr><td>Parent signed:</td><td>Date:</td></tr>
</table>

APPENDIX 1c - Acceptable use agreement (pupils and parents/carers) KS3- KS5

Acceptable use agreement (pupils and parents/carers)

Name of pupil:

These online safety rules help to protect students and the school by describing acceptable and unacceptable use of devices and systems (including computers, mobile devices and learning platforms).

Safe

- I will make sure that my internet use is safe and legal and I am aware that online actions have offline consequences.
- I know that people online aren't always who they say they are and that I must always talk to an adult before meeting any online contacts.
- I know that my use of school computers, devices and internet access, including on my own devices will be monitored to protect me and ensure I comply with the school's acceptable use policy, therefore all my use of the Internet, school's learning platform and other related technologies can be logged and be made available to my teachers.
- I understand the school can exercise its right to monitor the use of the school's devices and computer systems and learning platform, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/carer may be contacted. I understand that irresponsible use may result in the loss of my network or Internet access. By accepting this policy, I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Private

- I know I must always check my privacy settings are safe and private.
- I will think before I share personal information and/or seek advice from an adult.
- I will keep my password safe and private as my privacy, school work and safety must be protected.

Responsible

- I will only log on to the school network/ learning platform with my own username and password and accept that I am responsible for all activity carried out under my username.
- I will not access or change other people's files, accounts or information.
- I will only upload appropriate pictures or videos of others online and when I have permission.
- I know I must respect the school's systems and equipment and if I cannot be responsible then I will lose the right to use them and understand that it may incur replacement or repair fees if deliberately damaged or stolen
- I understand that any device that has been provided to me by the school is for my use only.
- I know that school computers and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I'm not sure if something is allowed then I will ask a member of staff.
- I will write emails and online messages carefully and politely; as I know they could be forwarded or seen by someone I did not intend.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I know that use of the school's ICT system for personal financial gain, gambling, political purposes, advertising or illegal purposes. is not allowed
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I understand that any on-line meeting links that are shared with me, such as for on-line lessons are for my

use only and I will not share these with anyone else.

- I understand that when I join an on-line meeting or lesson set up by the school that I must log in using my school account.
- I know that I must not record any lessons or meetings, using any means, such as using a phone or screen recording software.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.

Kind

- I know that bullying in any form (on and off-line) is not tolerated and I know that technology should not be used for harassment.
- I will not upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community I will always think before I post as once I upload text, photos or videos they can become public and impossible to delete.
- I will not use technology, including discussions forums to be unkind to people
- I will be polite and appreciate that other users might have different views to my own, exchange appropriate information and will share my ideas constructively..

Legal

- I know it can be a criminal offence to hack accounts or systems or send threatening and offensive messages.
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos or other material online.

Reliable

- I will always check that any information I use online is reliable and accurate.
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present

Report

- If I am aware of anyone trying to misuse technology then I will report it to a member of staff.
- I will speak to an adult I trust if something happens to either myself or another pupil which makes me feel worried, scared or uncomfortable.
- I know that I can visit www.thinkuknow.co.uk, www.childnet.com and www.childline.org.uk to find out more about keeping safe online.

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during the school day, in clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
-

Parent/Carer: • I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. • I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Pupil signed:	**Date:**
Parent signed:	**Date:**

APPENDIX 2 – acceptable use for staff including trustees, governors, supply and volunteers

CELT ICT & Media Acceptable Use Policy – Staff (including trustees, governors, supply and Volunteers)

Cornwall Education Learning Trust (CELT) provide a range of technologies (hereby referred to as "Information Services") including PC's, Laptops, mobile phones, tablets, digital cameras, Wired and Wireless Networks, Telecommunications, Email, social media sites, Applications, to support teaching and learning, data and data storage.. These technologies offer access to a vast amount of information which can be either locally stored, or available on remote networks such as the Internet.

Information Services are provided and maintained for the benefit of all CELT users (students, staff and visitors), and are intended to be freely available by all. It is a user's responsibility to access and use Information Services appropriately and only to aid teaching or learning, not for excessive recreation or personal gain. Access to Information Services must be within UK Law and specifically adhere to the terms set out in this policy.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that CELT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

CELT will try to ensure that staff and volunteers have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

As a professional organisation with responsibility for safeguarding it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are required to read and sign this Acceptable Use Policy. This is not an exhaustive list; all members of staff are reminded that ICT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the law.

Acceptable Use Policy Agreement

I understand that I must use CELT's systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

I recognise the value of the use of Information Services for enhancing learning and will ensure that pupils receive opportunities to gain from the use of information services. I will, where possible, educate the pupils in my care in the safe use of information services and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor the use of its Information Services, including email and other digital communications in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, the

school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

- I understand that the rules set out in this agreement also apply to use of CELT's Information Services outside of the academy.
- I understand that CELT's Information Services are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident that I become aware of, to my line manager.
- I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, or the school, into disrepute.

I will be professional in my communications and actions when using academy Information Services systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images.
- I will only use chat and social networking sites in the academy in accordance with the academy's policies. Use of social networking outside of CELT will be in line with professional standards and not bring the academy or myself in to disrepute. I will not add current or exstudents as 'friends' or communicate privately with them on social networking sites.
- I will only communicate with pupils and parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times.
    a. All communication will take place via school approved communication channels such as a school provided email address or telephone number, and not via personal devices or communication channels, such as personal email, social networking or mobile phones.
-
- I will not engage in any on-line activity that may compromise my professional responsibilities.

CELT has a responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my personal mobile / external devices (laptops / mobile phones / tablets / USB devices etc) in the academy, or access systems via Remote Access services at home, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password; a strong password consists of 8 or more characters which contain at least one character from three of the following character sets: number, upper case letter, lower case letter, symbol, and is only used on one system.
- I will apply software updates that have been deployed to my devices to ensure that software and operating systems are patched from vulnerabilities and up to date. I should not postpone the application of such software updates. Systems will update and reboot should such updates be continually postponed, therefore there is a risk to losing unsaved work if these updates are postponed.

- I will use appropriate email encryption systems to ensure sensitive information can only be read by the intended audience.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.
- I will ensure that my personal data is regularly backed up, in accordance with relevant academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering/ security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programs on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with The Data Protection Act and the school's Data Protection Policy.) This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data which is being removed from the school site must be encrypted by a method approved by the school.
    - Any images or videos of pupils will only be used as stated in the online safety policy and will always take into account parental consent.

    - The school's data protection lead must be informed in the event of any data being lost, stolen, or inadvertently disclosed. For example, a laptop is stolen or a mobile phone is lost with personal data stored on it.
- I understand that the data protection policy requires that any staff or pupil data to which I have access to will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will not store professional documents which contain school-related sensitive or personal information, including images, files, and videos, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible I will use the School's Office 365 platform, VPN or Remote Desktop systems to upload and access any work documents and files in a password protected environment.
- I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.
- I will only transport, hold, disclose or share personal information about myself or others, as instructed and in compliance with data protection laws and other academy policies.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- When using Remote Access services outside of the academy (at home or other external locations) I will be mindful of data protection issues and ensure that confidential or sensitive data is not seen by others, or left on screen unattended. I will always ensure I log off remote sessions when not in active use.
- I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the school's online safety lead.

When using the internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others.
- Where work is protected by copyright, I will not download or distribute copies (including pictures, music and videos).

I understand that I am responsible for my actions in and out of academy:
I understand that this Acceptable Use Policy applies not only to my work and use of Information Services equipment in academy, but also applies to my use of CELT's systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by CELT.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors, and in the event of illegal activities the involvement of the police.

I have read and understand the online safety policy which covers the requirements for safe IT use, including using appropriate devices, delivery of online lessons, safe use of social media and the supervision of pupils within the classroom and other working spaces. I also agree to the above and agree to adhere to the conditions set out in the Acceptable Use

Policy.

Name

School / Site

Signed

Date

Please return your completed forms to your office manager. Copies will be held digitally and centrally on file at your main base.

Wi-Fi Acceptable Use Policy (Guest and Bring your own device access)

As a professional organisation with responsibility for safeguarding it is important all members of the school community are fully aware of the School boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list; all members of the school community are reminded that ICT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the law.

All references to School include the school and Cornwall Education Learning Trust.

- The School provides Wi-Fi for the School community and allows temporary guest access for visitors and BYOD (Bring your own device) access for staff and sixth form pupils.
- I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of the school or is not part of a pupil 1 to 1 device scheme.
- The use of ICT devices falls under the school's Acceptable Use Policy and Online Safety Policy which all pupils, staff and other adults must agree to, and comply with.
- The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
- School-owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I will take all practical steps necessary to make sure that any equipment connected to the school's service is adequately secure, such as ensuring that connected equipment has up-to-date anti-virus software and system updates.
- Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorised use or access into my computer or device.
- The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.
- The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

- I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will not attempt to bypass any of the school's security and filtering systems or download any unauthorised software or applications.
- My use of the school Wi-Fi will be safe and responsible and will always be in accordance with this Acceptable Use appendix and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, web publications and any other devices or websites.
- I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
- I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the school's online safety lead, DSL or IT Support as soon as possible.
- If I have any queries or questions regarding safe behaviour online then I will discuss them with school's online safety lead, DSL, or the Headteacher.
- I understand that my use of the school's Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

APPENDIX 3 - Protocol for Online Communication

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

- 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.
- 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 - provided email accounts for educational purposes.
- All CELT staff are provided with a specific school 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'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.

APPENDIX 4 – 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 and understand the following:

- 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 Allegations Against Staff, Behaviour and Safeguarding/Child Protection.
- Any breaches of school 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 and Facebook.
- Each school/setting has their own official social media channels.
- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official school 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 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 Child Protection and Safeguarding.
- 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 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 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 on social media.

School 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, then they are requested to be professional at all times and are reminded that they are an ambassador for the school.

- 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.
- 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.

APPENDIX 5 - Use of Personal Devices and Mobile Phones

- The widespread ownership of mobile phones and a range of other personal devices among pupils 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 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 e.g. changing rooms.
- 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 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.
- In secondary schools, 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 except to enable MFA codes to be generated to ensure safe logon, permission to use mobile phones or devices can be sought from 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.

APPENDIX 6 -Protocol for Safer Use of Technology
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, nude and semi nude images, cyberbullying

and illegal content.

- 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 MARU or 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 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 Concern

Online Sexual Violence and Sexual Harassment between Children

- CELT schools and settings have accessed and understood part 5 of 'Keeping children safe in education' 2024

- 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 Child on Child 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.

The sharing of nude and semi-nude images
CELT recognises the sharing of nudes and semi-nudes (formerly known as "sexting"/youth produced sexual imagery) as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

CELT schools will follow the advice as set out in the non-statutory UKCCIS guidance: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudesadvice-for-education-settings-working-with-children-and-young-people/sharing-nudesand-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

CELT will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing nude and semi-nude images 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
CELT will respond to concerns, regardless of whether the incident took place on/off site
CELT will not:

- View any images suspected of being nude/semi-nude, 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 and will not allow or request pupils/young people to do so.

If made aware of an incident involving the creation or distribution of nude or semi-nude images, we will:

- act in accordance with our child protection policies and the relevant CELT Safeguarding procedures
- ensure the DSL (or deputy) responds in line with the DFE publication
- 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/young people, 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: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advicefor-education-settings-working-with-children-and-young-people/sharing-nudes-andsemi-nudes-advice-for-education-settings-working-with-children-and-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:

- 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), 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 and dealt with in line with our child on child abuse policy.

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also child on child policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. [Class teachers/form teachers] will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

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 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.