Children’s University Trust

Online Safety Policy

Review Date: December 2023

Approved by Trustees on: June 2022

Next Review Date: December 2024

You are advised that a printed version may not be the latest available version. The latest version, which supersedes all previous versions, is available on Board Effect. Those to whom this policy applies, are responsible for familiarising themselves with the latest version and for complying with the policy requirements at all times.

Page left blank intentionally

1. Rationale

Children's University Trust understands its responsibility to ensure safe use of information and communications technology (ICT) within our organisation. We believe that the child's welfare is paramount and note that:

*"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate."*Keeping Children Safe in Education (DFE 2023)

Children's University Trust recognises ICT is now an integral part of children's lives and provides them with access to a wide range of information and increased opportunities for instant communication and social networking. Using ICT can benefit children's education and social development, but it can also present several risks. Much ICT, particularly web-based resources, are not consistently policed and sometimes emerging risks are not fully understood. Children are often unaware that they are as much at risk online as they are in the real world and professionals may not be aware of the actions they can take to protect them. Children's University Trust aims to be fully aware of the range of risks associated with the use of these varied and emerging technologies and ensures that a range of protective measures are put into place to safeguard our organisation and the people who use our services. We are committed to developing an effective approach to online safety to empower staff and our member organisations to protect and educate children in their use of IT and establish mechanisms to identify, intervene and escalate any incident where appropriate. This policy aims to clarify the responsibilities of Children's University Trust staff when putting these protective measures in place.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

This policy is inclusive of both fixed and mobile internet; technologies provided by Children's University Trust (such as mobiles, laptops, notebooks, webcams, whiteboards, digital video equipment, etc.); and technologies owned by Children's University Trust staff, but brought onto any Children's University Trust premises (such as laptops, notebooks, mobile phones, camera phones and portable media players, etc.).

The term 'staff' in this policy will mainly be used to refer to: paid staff, volunteers, anyone undertaking work experience or a work placement with Children's University Trust and our Trustees; 'parents' will include 'carers', and 'children' will include children and young people up to the age of 18.

2. Aims

Children’s University Trust aims to:

- fulfil our legal duties in regard to online safety and Data Protection
- promote the safe use of ICT as a useful educational tool within our organisation
- understand the risks inherent in the use of ICT and safeguard the welfare of children
- protect the reputation of Children’s University Trust
- ensure the security of our ICT systems
- ensure appropriate filters and appropriate monitoring systems are in place
- meet the needs of all children and ensure that all children have equal access to ICT
- ensure that the Trust works within the law and statutory guidance in regard to ICT and data; and
- keep up to date with new developments and new risks in the field of ICT and put appropriate protectives measures in place as necessary.

3. Related Policies
This policy works in conjunction with the following Trust policies:

- Antibullying
- Complaints
- Equalities
- Privacy
- Safer Recruitment
- Safeguarding and Child Protection; and
- Whistleblowing.

4. Law and Guidance
This policy works within the following legal framework and statutory guidance:

Legal Framework:
Access to Medical Reports Act 1988
Data Protection Act, 1998 Public Interest Disclosure Act, 1998
Freedom of Information Act 2000
Access to Medical Records Act 1988
Equality Act 2010
Transfer of Undertakings (Protection of Employment) Regulations 2006
Data Protection Act 2018

Statutory Guidance:
Working Together to Safeguard Children (2018)
Keeping Children Safe in Education (2023)
Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers (2018)

5. Leadership

(i) Online Safety Coordinator
Children’s University Trust designates as Online Safety Coordinator:

The duties of the Online Safety Coordinator include:

- review the Online Safety Policy and procedures;

- provide the first point of contact and advice for Trust staff, trustee, children and parents about online safety matters;
- liaise with our IT supplier to ensure they are kept up to date with online safety issues and advise of any new trends, incidents and arising problems to the Trustees
- raise the profile of online safety awareness within the Trust by giving advice and ensuring access to training and relevant online safety literature when appropriate
- ensure that all staff are aware of online safety policies at Induction and in particular the procedures that need to be followed in the event of an online safety incident taking place
- maintain a file of internet related incidents and co-ordinate any investigation into breaches
- meet regularly with the Trustees to discuss current issues
- liaise with any online safety meetings as necessary
- ensure data management in Children's University Trust complies with legislation
- answer queries of staff or children on policy and practice
- respond to complaints; and
- assess, as far as is reasonably practicable, the impact and risk of emerging technology (e.g. a new social networking website).

(ii) Trustees

The duties of the Children's University Trust Trustees in regard to online safety include:

- approve the Online Safety Policy
- consider a whole organisational approach to online safety
- manage risks
- make reports where necessary to the police, social services and other agencies, and when the criteria are met, send a serious incident report to the Charity Commission
- support the work of the Online Safety Coordinator; and
- ensure that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.

(iv) All staff and Trustees

All Children's University Trust staff and Trustees have the duty to:

- work within this Online Safety Policy and related online safety policies
- sign the Acceptable Use of ICT agreement; and
- report any online safeguarding concerns to the DSL.

6. Implementation

This policy is the responsibility of everyone who works or volunteers at Children's University Trust. The DSL and the Trustees will ensure that arrangements will be made to bring this policy to the notice of all staff (including new, temporary, and part-time staff), agency and other contract staff, volunteers and children in an appropriate manner to their age, so that they fulfil their duties to co-operate with this policy.

7. Review

This online safety Policy and its implementation shall be reviewed annually.

8. Online Safety Procedures

8.1 Communication

All communication with children and families by staff should be transparent and open to scrutiny. Children's University Trust staff should not request or respond to any personal information from children and parents other than which may be necessary in their professional role. Trust staff should aim to not give their personal contact details to children for example: email address, home or mobile telephone numbers, details of web based identities. Contact with children using ICT should be mediated through or include parents, and membership organisation staff, unless there are particular circumstances that necessitate direct contact (e.g. use of mobile phones during outings, residential trips or festivals). This communication should be planned carefully and requires a Risk Assessment carried out by the relevant Children’s University Trust Manager. Essential communication with children should be agreed in advance with management and copy in the parents. Video conferencing during sessions with children will not be used. **If children attempt to contact or correspond with Trust staff directly or indirectly for personal reasons using social media or any other technology, staff should not respond and must report the matter to the DSL.**

8.2 Complaints

Complaints of ICT misuse will be dealt with by a senior member of staff. Any complaint about Children’s University Trust staff misuse must be referred to the Online Safety Coordinator. Complaints involving a safeguarding concern shall be dealt with in accordance with the Trust’s Safeguarding Policy. Parent and carers will be informed of the complaints procedure. Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

8.3 Computers

Children’s University Trust staff are only permitted access to parts of the computer system, which are necessary in order to carry out their normal activities, or authorised for personal use. The following examples constitute computer misuse:

- Fraud and theft
- Introduction of viruses
- Loading and/or using unauthorised software
- Obtaining unauthorised access
- Using the system for non-work related activities or non-authorised activities, including games during work time. (Use of the system outside work time is permitted, providing the employee has received authorisation from the CEO)
- Breach of the Trust’s Privacy Policy.

Children’s University Trust staff should not use Trust computers for personal use. All files that contain personal data will be stored appropriately and securely in accordance with the Trust Data Protection Policy, e.g. password protected or locked away. Staff should not forward any Trust work, files, information etc. stored on Trust computers/laptops to their home computer, unless this has been agreed by the CEO as necessary. Caution should be taken if personal email addresses are used on Trust computers within settings. Illegal or inappropriate materials must not be uploaded, downloaded or accessed.

8.4 Confidentiality

Trust staff may have access to confidential information about children which must be kept confidential at all times and only shared when legally permissible to do so and in the interest of the child. Records should only be shared with those who have a legitimate professional need to see them.

8.5 Data Protection

Children’s University Trust is aware that among other obligations, the Data Protection Act 2018 and the GDPR place duties on organisations and individuals to process personal information fairly and lawfully and to keep the information they hold safe and secure. We also understand that the Data Protection Act 2018 and GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children or adults with care and support needs safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children and adults with care and support needs. Trust staff are expected to comply with the Trust’s Privacy Policy. Any breaches of this may result in disciplinary action. Staff may at times have access to confidential and sensitive information and have a duty of confidentiality to the Trust and its clients. Information an employee receives in the course of their job must not be used for their own benefit or the benefit of others, and must not be disclosed to anyone outside the Trust, except in cases of whistleblowing. Children’s full names/names will not be used anywhere on the Trust’s literature. We will store children’s personal information for the entire period that an organisation is partnered with us, and may retain these details in accordance with our Privacy Policy.

8.6 Email

Email and the internet are available for communicating on Children’s University Trust business. The following provisions for use of email and the internet also apply to access provided for remote use (e.g. hand- held, portable devices etc.) and to home working staff using their own IT equipment outside of Trust premises during working time or whilst undertaking Children’s University Trust duties. Staff attention is drawn to the fact that external email is not secure and that this must be taken into account in choosing how personal and confidential information is communicated. Staff must ensure that they do not make inappropriate comments in any emails. They should be aware that contracts formed by email or over the internet might be legally binding. Any contractual agreement, offer or acceptance must only be made by an employee via email or over the internet where either the employee has authority to do this or where specific line-management authorisation has been given. It is recognised that from time to time, email and internet facilities may be used for personal reasons unrelated to Trust business. Such use should be brief, outside of working hours (except in a case of emergency) and must exclude activities prohibited by the Trust. Excessive personal use of email or the internet is unacceptable and appropriate disciplinary action will be taken. Sharing personal email accounts is not allowed to parents or to partner organisations. Emails sent to any external organisations should be written carefully and authorised if sensitive before sending, in the same way as a letter written on Childrens’ University Trust headed paper. Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

8.7 Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Trust.

8.8 Intellectual Property

Intellectual Property is a generic legal term, which refers to the rights and obligations received and granted (including copyright) in relation to, for example: inventions, patents, creative writings and drawings (including policy, training and technical documents and materials). If an employee creates these during the course of their employment, then the copyright in the item belongs to the Trust.

8.9 Internet

The internet is an essential element for education, business and social interaction. There are many risks, however, associated with abusive and dangerous web material that is easily accessible. Children’s University Trust will ensure that internet access used within our organisation by children will have appropriate content filtering. The use of internet derived materials by staff and Children’s University participants should comply with copyright law. All staff should read and sign the Children’s University Trust ‘Acceptable ICT Use Agreement’ (in the Appendix) before using ICT as a resource.

8.10 Mobile Phones and other mobile devices

Most mobile phones now have access to the internet and picture and video messaging and may present opportunities for unrestricted access to the internet and sharing of images. Other mobile devices with this facility include laptops, tablets, watches and gaming hardware.

Generally, Children’s University Trust staff should use the telephone or other mobile devices for business use only while at work. Personal mobile phones and other devices may be used in some situations, as long as it is for business and emergency purposes only and staff are not to be distracted. Staff are responsible for keeping their own mobile devices up to date through software, security and app updates. The device should be virus protected and should not be capable of passing on infections to the Children’s University Trust network. Staff are responsible for charging their devices and for protecting and looking after their devices and will be held responsible for the upkeep, content and security of their own devices, e.g. access to web pages. If this is deemed to be a safeguarding issue this will be dealt in accordance with our safeguarding and management policies.

When working in a partnership setting, staff must use mobile devices in accordance with the policy of the setting. This may include not bringing in a mobile device at all, or handing in the device at reception. The Trust recognises that in exceptional circumstances it is necessary for staff to make or receive personal calls, emails or SMS during working hours. In these circumstances any personal usage should be brief, and where possible made in the employee's work breaks. Printing from personal devices will not be possible.

Children’s University Trust staff must never exchange mobile phone numbers with any children unless there is a specific purpose which may entail a risk assessment.

Staff are not to use any mobile phone cameras to photograph children, unless, there is a specific purpose which may entail a risk assessment and parental permission is obtained. Images taken of children should be downloaded onto the Trust’s computers only and not be downloaded onto any personal device.

8.11 Personal Websites and Blogs
Children’s University Trust staff who wish to set up personal web forums, weblogs or 'blogs' must do so outside of work, not use Trust equipment, and adhere to the points detailed in this policy.

8.12 Photography and recordings
Pictures, videos and sounds are easily transferred and pose a real safeguarding issue to children. Children’s University Trust will ensure that the publishing of images, video and sound will follow the policy set out in the Privacy policy. If photographs or videos are required (e.g. recording graduations for marketing material or for a specific project or event), this must be arranged in agreement with the DSL, children, parents and all partner organisations including schools. Children’s University Trust will ensure that all relevant publicity permissions have been received for the relevant event and any relevant risk assessment undertaken. **Written permission from parents and/or Children’s University Trust member organisations will be obtained before photographs of children are published.** Parents or partnerships may withdraw permission at any time. All images are stored in line with the Privacy Policy. Parents should not use digital cameras, mobile phones or video equipment during events unless specifically authorised. In this case, Children’s University Trust or membership organisation staff should inform parents and others present that photographs and videos may be taken on the basis that they are for private retention and not for publication in any manner. Parents may upload pictures of their own child only onto social networking sites. If the picture includes another child then it is their responsibility to gain permission from that child’s parents.

8.13 Security

Children’s University Trust is committed to ensuring that all its ICT systems are as secure as possible. We will ensure that:

- ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with our system provider and arrangements incorporated in our agreement with them
- Personal data will be recorded, processed, transferred and made available according to legislation.

All reasonable precautions will be taken to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a Children’s University Trust device. We do not accept liability for the material accessed, or any consequences of Internet access.

8.14 Site specific considerations
Children’s University Trust staff must adhere to the policies of partner organisations including schools in the use of ICT across different sites, and they must specifically check about online safety arrangements as part of their work. If they are allowed to keep their phones on them, we recommend that staff switch their mobile phones to silent, and do not use whilst participating in or observing activities. All personal devices should be restricted through the implementation of technical solutions that provide appropriate levels of network access. We accept no responsibility or liability in respect of lost, stolen or damaged devices and recommend insurance is purchased by staff to cover damage. We accept no responsibility for any malfunction of a device due to changes made to the device while on the partnership networks or elsewhere or whilst resolving any connectivity issues. Pass-codes or PINs should be set on personal devices to aid security. ICT which has the capability to take videos or photographs should not be used by staff with children unless their use has been cleared by the partner organisation and the DSL prior to use. Personal devices should be charged before being brought to partner organisations. We recommend our partner organisations have the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate. We recommend that all partner organisations using ICT with children within sessions gain parental permission for this.

8.15 Social Networking
Children’s University Trust respects an employee's private life. However, it must also ensure that confidentiality and its reputation are protected. Staff using social networking websites in their private life must refrain from promoting themselves as working for the Trust, in a way which has, or may have, the effect of bringing the Trust into disrepute. They must not identify other Trust staff, partner organisations or service users without their consent, must not make any defamatory remarks about them or conduct themselves in a way that is detrimental to the Trust. Staff must not disclose personal data or information about Children’s University Trust, staff, partner organisations or service users that could breach legislation. (e.g. photographs, images). Staff should not engage in any online activity or communication with children and families. They should be aware of possible wider implications when entering any personal details on any online sites. If children attempt to contact or correspond with staff directly or indirectly for personal reasons using social media, staff should not respond and must report the matter to the DSL.

8.16 Website
The Children’s University website is a valuable source of information for children and parents, but it must be managed to reduce any potential risks. The DSL will take overall safeguarding editorial responsibility and ensure that website content is accurate and appropriate. The Trust must ensure

that staff and all service user’s personal information will not be published on the website, particularly names in association with photographs. Photographs and videos that include children will be selected carefully and will not enable individual children to be clearly identified, and consent from parents or carers will be obtained before photographs are published on the website.

9. Safeguarding concerns relating to online safety

9.1 Cyber bullying

Current government guidance ‘Preventing and Tackling Bullying’ (2017) defines bullying as:

‘…behaviour by an individual or group, repeated over time, that intentionally hurts another individual or group either physically or emotionally. Bullying can take many forms (for instance, cyber-bullying via text messages, social media or gaming, which can include the use of images and video) and is often motivated by prejudice against particular groups, for example on grounds of race, religion, gender, sexual orientation, special educational needs or disabilities, or because a child is adopted, in care or has caring responsibilities. It might be motivated by actual differences between children, or perceived differences.’

Bullying can seriously damage someone’s confidence and self-esteem. It can lead to serious and prolonged emotional damage for an individual. Those who conduct the bullying can also experience emotional harm. The impact on parents and carers and staff can also be significant. Bullying is therefore a key safeguarding concern. It is important that incidents of bullying are distinguished from isolated incidents. Bullying is considered to be repeated violence, mental or physical, conducted by an individual or a group and directed against other individuals. Bullying can take place between children, between children and staff, or between staff. Bullying can occur for a variety of reasons, all of which should be taken equally seriously and dealt with appropriately. Bullying occurs online through messaging and social networking sites. Any employee who feels that a participant has been a victim of bullying should report their concern to the DSL on the same day it is noted.

9.2 Child Criminal Exploitation (County Lines)

Criminal exploitation of children is a geographically widespread form of harm that is a typical feature of county lines criminal activity: drug networks or gangs groom and exploit children and young people to carry drugs and money from urban areas to suburban and rural areas, market and seaside towns. Key to identifying potential involvement in county lines are missing episodes, when the victim may have been trafficked for the purpose of transporting drugs and a referral to the Police should be considered. Children are manipulated and monitored using ICT. County lines exploitation:

- can affect any child or young person (male or female) under the age of 18 years
- can still be exploitation even if the activity appears consensual
- can involve force and/or enticement-based methods of compliance and is often accompanied by violence or threats of violence
- can be perpetrated by individuals or groups, males or females, and young people or adults; and
- is typified by some form of power imbalance in favour of those perpetrating the exploitation.

Whilst age may be the most obvious, this power imbalance can also be due to a range of other factors including gender, cognitive ability, physical strength, status, and access to economic or other resources.

Any employee who feels that a Children’s University participant has been a victim of criminal exploitation should report their concern to the DSL on the same day it is noted.

9.3 Child Sexual Exploitation and Trafficking (CSE)
CSE is a form of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial advantage or increased status of the perpetrator or facilitator. The victim may have been sexually exploited even if the sexual activity appears consensual. CSE does not always involve physical contact; it can also occur through the use of technology. Signs of CSE include:

- Children who appear with unexplained gifts or new possessions;
- Children who associate with other young people involved in exploitation;
- Children who have older boyfriends or girlfriends;
- Children who suffer from sexually transmitted infections or become pregnant;
- Children who suffer from changes in emotional well-being;
- Children who misuse drugs and alcohol;
- Children who go missing for periods of time or regularly come home late; and
- Children who regularly miss partnership or education or don't take part in education.

Some young people are groomed through 'boyfriends' who then force them into having sex with others. On rare occasions young people can be trafficked over different parts of the country by organized gangs of exploiters. Any employee who feels that a Children's University participant has been a victim of CSE should report their concern to the DSL on the same day it is noted.

9.4 Grooming
Grooming is when someone builds an emotional connection with a child or young person to gain their trust for the purposes of sexual abuse or exploitation. Children can be groomed online by a stranger or by somebody they know. Groomers may be male or females and could be any age, and many children and young people don't understand they have been groomed, or that what has happened is abuse. The groomer will hide their true intention and may spend a long time gaining a young person's trust. Once they have established trust, groomer will exploit the relationship by isolating the victim from friends or family and making the victim feel dependent upon them. Groomers no longer need to meet victims in real life to abuse them and can use social media sites, instant messaging apps including teen dating apps, or online gaming platforms to connect with a young person or child. Groomers can hide their identity online, they may pretend to be a child and then chat and become 'friends' with victims they are targeting. Groomers may look for:

- User names or comment that are flirtatious or have a sexual meaning; and/or
- Public comments that suggest a child has low self-esteem or is vulnerable.

Any employee who feels that a Children's University participant has been a victim of grooming should report their concern to the DSL on the same day it is noted.

9.5 Peer Abuse
Children's University Trust recognises that children are capable of abusing their peers. Peer abuse is abuse and should never be tolerated or passed off as "banter" or "part of growing up". Peer on peer abuse can take many forms, and can manifest itself in many ways, including sexting, online abuse, bullying and cyber bullying and sexual abuse. We recognise that peer abuse is frequently gendered. Girls are more likely to be sexually touched or assaulted and boys are more likely to be subject to initiation/hazing type violence. Accordingly allegations of peer on peer abuse will be taken extremely seriously and investigated and dealt with. Any employee who feels that student has been a victim of peer abuse should report their concern to the DSL on the same day it is noted.

9.6 Radicalisation

From 1 July 2015 all registered providers of education are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, to have “due regard to the need to prevent people from being drawn into terrorism”. Although Children’s University Trust is not a registered provider, we do work closely with schools and other registered providers and we therefore are addressing Prevent Duties within our organisation as part of our wider safeguarding responsibilities to protect children from harm. The internet provides people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. We will ensure that children are safe from terrorist and extremist material when accessing CU Online and ensure that suitable filtering is in place. We will help children with the skills to stay safe online, both in the settings we work in and outside. Where staff, children or visitors find unblocked extremist content they must report it to the DSL. We are aware that children have access to unfiltered internet when using their mobile phones and staff should be alert to the need for vigilance when they are using their phones. The Trust is committed to identifying people who may be vulnerable to radicalisation. Early indicators of radicalisation or extremism may include out of character changes in dress, behaviour and peer relationships (although there are also very powerful narratives, programmes and networks online so involvement with particular groups may not be apparent); secretive behaviour; and online searches or sharing extremist messages or social profiles. Staff with concerns that children are becoming radicalised should contact the DSL the same day the concern is noted. As well as contacting the local safeguarding referral agency, the DSL should also contact the local Counter Terrorism Intelligence Unit. If there is a terrorist related emergency, staff should contact the Police immediately.

9.7 Sexting

'Sexting' is the exchange of self-generated sexually explicit images, through mobile picture messages or webcams over the internet. Young people may also call it:

- cybersex
- sending a nudie, picture or selfie
- trading nudes
- dirtie; and
- pic for pic.

There are many reasons why a child may want to send a naked or semi-naked picture, video or message to someone else. These reasons include:

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

Sexting is often seen as flirting by children and young people who feel that it's a part of normal life, but in fact it is a crime. The law in the UK currently states that the creating or sharing explicit images of a child is illegal, even if the person doing it is a child. As of January 2016, if a young person is found creating or sharing images, the police can choose to record that a crime has been committed but that taking formal action isn't in the public interest. In addition crimes recorded this way are unlikely to appear on future records or checks, unless the young person has been involved in other similar activities which may indicate that they're a risk. Any employee who feels that a Children’s University participant has been involved in sexing should report their concern to the DSL on the same day it is noted.

9.8 Sexual Abuse

Sexual abuse is defined as: 'forcing or enticing a child to take part in sexual activities, whether or not the child is aware of what is happening.' The activities may involve physical contact, including penetrative (e.g. rape, buggery) or non-penetrative acts (kissing, rubbing, masturbation, touching on outside of clothing). Sexual abuse Includes grooming by the Internet. Signs and symptoms of sexual abuse include:

- Being overly affectionate or knowledgeable in a sexual way
- Medical problems such as chronic itching, pain in the genital, venereal diseases
- Other extreme reactions, such as depression, self-mutilation, suicide attempts, overdoses, anorexia
- Personality changes such as becoming insecure or clinging
- Regressing to younger behaviour patterns such as thumb sucking or bringing out discarded cuddly toys
- Sudden loss of appetite or compulsive eating
- Being isolated or withdrawn
- Inability to concentrate
- Lack of trust or fear of someone they know well
- Become worried about clothing being removed
- Suddenly drawing sexually explicit pictures
- Trying to be 'ultra-good' or perfect; overreacting to criticism.

Concerns that any child is being sexually abused should be reported to the DSL on the same day they are noted.

10. Appendices

Appendix 1	Acceptable Use of ICT Agreement - staff

Children’s University
Acceptable Use ICT Agreement – staff and trustees

ICT and the related technologies such as email, the internet, iPads and mobile phones are an expected part of our daily working life at Children’s University Trust. This policy is designed to ensure that everyone is aware of their responsibilities when using any form of ICT. All users of ICT within Children’s University Trust are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Children’s University Trust’s Online Safety Co-ordinator.

- I will only use Children’s University Trust’s email/internet and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the Trustees
- I will comply with the ICT system security and not disclose any passwords provided to me by Children’s University Trust or other related authorities
- I will ensure that all electronic communications with children and staff are compatible with my professional role
- I will only use the approved, secure email system(s) for any Children’s University Trust business
- I will ensure that personal data is kept secure and is used appropriately, whether in the Children’s University Trust, taken off any Trust premises or accessed remotely
- I will not browse, download or upload material that could be considered offensive or illegal
- I will not send to children or colleagues material that could be considered offensive or illegal
- Images of children will only be taken and used for professional purposes and will not be distributed outside the Trust’s network without consent of the parent/carer
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to Children’s University Trust
- I will respect copyright and intellectual property rights
- I will support and promote the Children’s University Trust’s Online Safety Policy and help everyone to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe use of ICT throughout Children’s University Trust.

Staff Signature……………………………………………. Date……………………….

Print Name…………………………………………………