7 Gen
Analytics

Children's Safeguarding Policy for 7 Gen Analytics

www.7genanalytics.com

Children’s Safeguarding Policy for 7 Gen Analytics

Named personnel with designated responsibility for Child Protection

Year	Designated Senior Person	Deputy Designated Senior Person	Date approved	Review Date
2021	Brandon Bell	Sally Zaranko	23 july 2021	July 2022

Contents

Introduction:

This document has been created utilising best practice guidance for the protection of children from the following organisations and many others.

Camden

Camden Safeguarding Children Partnership

NSPCC
Cruelty to children must stop. FULL STOP.

Our Duty of Care:

7 Gen Analytics abides by the duty of care to safeguard and promote the welfare of children and young people and is committed to safeguarding practice that reflects statutory responsibilities, government guidance and complies with best practice requirements.

- We recognise the welfare of children is paramount in all the work we do and in all the decisions we take
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation has an equal right to protection from all types of harm or abuse
- Some children are additionally vulnerable because of the impact of previous experiences, their level of dependency, communication needs or other issues
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare.

Purpose:

7 Gen Analytics will:

- Protect children and young people who receive 7 Gen Analytics's services from harm. This includes the children of adults who use our services
- Provide staff and volunteers, as well as children and young people and their families, with the overarching principles that guide our approach to child protection.

This policy applies to anyone working on behalf of **7 Gen Analytics**, including senior managers and the board of trustees, paid staff, volunteers, sessional workers, agency staff and students. Failure to comply with the policy and related procedures will be addressed without delay and may ultimately result in dismissal/exclusion from the organisation.

Definitions:

The Children Act 1989 definition of a child is: anyone who has not yet reached their 18th birthday, even if they are living independently, are a member of the armed forces or are in hospital.

Adult at Risk:

- An adult who has needs for care and support (whether or not the authority is meeting any of those needs),
- is experiencing, or is at risk of, abuse or neglect, and
- as a result of those needs is unable to protect himself or herself against the abuse or neglect or the risk of it.

Child and Adult Abuse: Children and adults may be vulnerable to neglect and abuse or exploitation from within their family and from individuals they come across in their daily lives. There are 4 main categories of abuse, which are: sexual, physical, emotional abuse, and neglect. It is important to be aware of more specific types of abuse that fall within these categories, they are:

- Bullying and cyberbullying
- Child sexual exploitation
- Child Criminal exploitation
- Child trafficking
- Domestic abuse
- Female genital mutilation
- Grooming
- Historical abuse
- Online abuse

Safeguarding children: Safeguarding children is defined in Working Together to Safeguard Children 2018 as:

- protecting children from maltreatment.
- preventing impairment of children's health or development.

- ensuring that children are growing up in circumstances consistent with the provision of safe and effective care.
- taking action to enable all children to have the best outcomes.

Safeguarding:

In safeguarding children, 7 Gen Analytics is committed to the principles of Camden's Children Safeguarding Partnership.

Legal Framework:

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. A summary of the key legislation is available from nspcc.org.uk/learning.

7 Gen Analytics have in place arrangements that reflect the importance of safeguarding and promoting the welfare of children and young people as well as vulnerable adults.

The Prevent duty:

Some organisations in England, Scotland and Wales have a duty, as a specified authority under section 26 of the Counterterrorism and Security Act 2015, to identify vulnerable children and young people and prevent them from being drawn into terrorism. This is known as the Prevent duty. These organisations include:

- Schools
- Registered childcare providers
- Local authorities
- Police
- Prisons and probation services
- NHS trusts and foundations.
- Other organisations may also have Prevent duties if they perform delegated local authority functions.

Children can be exposed to different views and receive information from various sources. Some of these views may be considered radical or extreme.

Radicalisation is the process through which a person comes to support or be involved in extremist ideologies. It can result in a person becoming drawn into terrorism and is in itself a form of harm.

Extremism is vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs.

Training and Awareness:

7 Gen Analytics will ensure an appropriate level of safeguarding training is available to its Trustees, Employees, Volunteers and any relevant persons linked to the organisation who requires it (e.g. contractors).

For all employees who are working or volunteering with children, this requires them as a minimum to have awareness training that enables them to:

- Understand what safeguarding is and their role in safeguarding children.
- Recognise a child potentially in need of safeguarding and take action.
- Understand how to report a safeguarding Alert.
- Understand dignity and respect when working with children.
- Have knowledge of the Safeguarding Children Policy.

In the case of Camden our team will be undertaking the free training provided by the Camden's Children Safeguarding Partnership (CCSP)

Based upon CCSP's training analysis our team will need to achieve group 1 or potentially group 2 training dependent on role.

Our team will register **here** for the virtual training if required.

Training course	Purpose	Mode	person completing course	date complete
KCSIE Part 1	Basic awareness in child protection	Online		
Prevent	This offers an introduction to the Prevent duty, and explains how it aims to safeguard vulnerable people from being radicalised to supporting terrorism or becoming terrorists themselves.	Online		

Channel Awareness	Channel provides support to individuals who are vulnerable to being drawn into any form of terrorism. They aim is to divert that person from their path of radicalisation before they become involved in any terrorist-related criminal activity.	Online		
Working Together to Safeguard Children	A guide to inter-agency working to safeguard and promote the welfare of children	Document		

Similarly, employees and volunteers may encounter concerns about the safety and wellbeing of an adult at risk of abuse. For more information about adults safeguarding, refer to **7 Gen Analytics** Adults Safeguarding Policy.

Confidentiality and Information Sharing:

7 Gen Analytics expects all employees, volunteers and trustees to maintain confidentiality. Information will only be shared in line with the General Data Protection Regulations (GDPR) and Data Protection.

However, information should be shared with the Local Authority if a child is deemed to be at risk of harm or **contact the police if they are in immediate danger, or a crime has been committed**. For further guidance on information sharing and safeguarding see 7 Gen Analytics GDPR Policy.

What is confidentiality in safeguarding?

Confidentiality is an important principle that enables people to feel safe in sharing their concerns and to ask for help. However, the right to confidentiality is not absolute. Sharing relevant information with the right people at the right time is vital to good safeguarding practice.

Recording and Record Keeping Policy:

A written record must be kept about any concern regarding an adult with safeguarding needs. This must include details of the person involved, the nature of the concern and the actions taken, decisions made and why they were made.

All records must be signed and dated. All records must be securely and confidentially stored in line with General Data Protection Regulations (GDPR).

Our policy is based on the NSPCC guidance and the following protocols will be adhered to in the event of an incident.

- the date and time of the incident/disclosure:
- the date and time of the report
- the name and role of the person to whom the concern was originally reported and their contact details
- the name and role of the person making the report (if this is different to the
- above) and their contact details
- the names of all parties who were involved in the incident, including any witnesses
- the name, age and any other relevant information about the child who is the subject of the concern (including information about their parents or carers and any siblings)
- what was said or done and by whom
- any action taken to look into the matter
- any further action taken (such as a referral being made)
- the reasons why the organisation decided not to refer those concerns to a
- statutory agency (if relevant).

Make sure the report is factual. Any interpretation or inference drawn from what was observed, said or alleged should be clearly reported as such. The record should always be signed and dated by the person making the report.

Safe Recruitment & Selection:

7 Gen Analytics is committed to safe employment and safe recruitment practices that reduce the risk of harm to children from people unsuitable to work with them or have contact with them.

We ensure that all appropriate measures are applied in relation to everyone who works in or on behalf of 7Gen Analytics who is likely to be perceived by the children as a safe and trustworthy adult and follow guidance on checking volunteers and contractors.

Safer recruitment practice includes scrutinising applicants, verifying identity and academic or vocational qualifications, obtaining professional and character references, checking previous employment history and ensuring that a candidate has the health and physical capacity for the job. When undertaking interviews, the school has regard to the principles of Value Based Interviewing, guidance can be accessed via www.nspcc.org.uk.

Where appropriate, 7Gen analytics undertakes checks of/has regard to:

- the Disclosure and Barring Service (DBS)
- the Teacher prohibition list
- All staff are made aware that they are required to notify their line manager of any convictions or cautions during employment with the Council or if they receive a Penalty Notice for Damage or a Penalty Notice for Disorder. For those who drive on business at any point during their employment (company's vehicle or own vehicle), this includes all motoring offences dealt with through the courts and penalty points on driving licences - whether awarded by a court or through fixed penalty notices.
- An Enhanced DBS check is obtained for all new paid appointments to 7 Gen Analytics workforce where risk assessment deems necessary. e.g. financial staff will not have access to sensitive information
- An Enhanced DBS check is obtained for volunteers further to a risk assessment considering the regularity, frequency, duration and nature of contact with children and the level of supervision of the volunteer by another person engaging in regulated activity (KCSIE 2020).

DBS Register:

7 Gen Analytics holds a register of Disclosure and Barring Service checks for all employees that have access to children or data relating to children.

The register can be found **HERE.**

Social Media:

All employees and volunteers should be aware of **7 Gen Analytics** social media policy and procedures and the code of conduct for behaviour towards the children we support.

Online safety risks for young people can include, but are not limited to:

- making themselves identifiable by posting personal details on social media such as the school they attend or their home address
- communicating with people they don't know, including potentially dangerous individuals
- potential for inappropriate relationships between adults in positions of trust, or influence and the young people they work with
- sexual grooming, luring, exploitation and abuse, or unwanted contact
- exposure to inappropriate content, including pornography, racist or hate material or violent behaviour
- being encouraged to create or share inappropriate or harmful material of themselves or others, including sexting (sexual images or video)
- glorifying activities such as drug taking or excessive drinking
- cyberbullying or berating by peers and people they consider 'friends' – in sport this can include negative comments or reactions about their performance or achievement
- access to inaccurate and therefore potentially harmful information
- encouragement to take part in violent behaviour or harmful trends

Use of Mobile Phones and other Digital Technology:

As with online safety issues generally, risks to children and young people should be broadly categorised under the headings of:

- content
- contact
- conduct
- commerce

All employees, trustees and volunteers should be aware of **7 Gen Analytics** policy and procedures regarding the use of mobile phones and any digital technology and understand that it is unlawful to photograph children and young people without the explicit consent of the person with parental responsibilities.

Use of mobile phones and cameras Photographs will only be taken of children with their parents' permission. Only the business cameras will be used to take photographs of children except with the express permission of the manager. **Neither staff nor children nor visitors may use their mobile phones to take photographs.**

This section should be read in conjunction with Appendix B and the following Considerations for management document found here.

Whistleblowing:

It is important that people within **7 Gen Analytics** have the confidence to come forward to speak or act if they are unhappy with anything. Whistle blowing occurs when a person raises a concern about dangerous or illegal activity, or any wrong-doing within their organisation. This includes concerns about another employee or volunteer. There is also a requirement by **7 Gen Analytics** to protect whistleblowers. https://www.gov.uk/whistleblowing

Appendix A: Important Contacts:

Senior Lead for Safeguarding	
Name:	Brandon Bell
Email address:	brandon@7genanalytics.com
Telephone number:	
Deputy Senior Lead for Safeguarding	
Name:	Sally Zaranko
Email address:	sally@7genanalytics.com
Telephone number:	
Trustee for Safeguarding	
Name:	
Email address:	
Telephone number:	
Police	Emergency – 999 Non-emergency – 101
NSPCC Helpline	0808 800 5000

Appendix B: Guidelines for Safe Use of Digital Technology in Child Care Settings

Introduction

This guidance has been produced for early years settings, including nurseries, pre-schools, childminders and out of school clubs and complements the broader Education e safety Policy Guidance referred to below. It is intended to give practical advice to staff and volunteers in safeguarding children from the possible risks associated with digital technology as well as ensuring that staff protect themselves through safe and responsible working practices. This guidance should be made available to parents and carers and should be regularly updated. The guidance includes acceptable use policies and agreements as well as photography and video permission.

New technologies open up many exciting benefits and opportunities for learning and development but can also present risks. Wider access to technology via iPads/tablets, mobile phones, games consoles and other devices bring new challenges about controlling access and content. The Enfield Education e safety policy provides a detailed overview together with recommended strategies and resources for education providers, parents and children and young people.

Although children within Early Years Settings will not normally be accessing technology independently and benefit from a high level of supervision, there is always a small element of risk. Safeguarding is everyone's responsibility and all providers have a role in helping children stay safe on line and supporting the adults who work with children in minimising risks.

The value of ICT as a learning tool is embedded within the Early Years Foundation Stage. Early years practitioners and managers should therefore support children and young people in using a range of ICT (resources) which may include cameras, photocopiers, CD players, tape recorders and programmable toys in addition to computers. Early Years practitioners and their managers should also be able to support children and young people to talk about ICT apparatus, what it does, what they can do with it and how to use it safely. It is also important for parents and carers to be fully involved with promoting online safety within the setting, home and social environment.

E safety responsibilities for providers include technological infrastructure, filtering and monitoring systems, recognition and responses to e safety concerns plus ongoing risk assessment to identify emerging issues.

Safer Working Practice is essential as although most people who work with children have their best interests at heart, we know that sadly some people have abused their position of trust to abuse children in ways that have been further amplified through the digital environment. This should therefore be seen as part of the broader responsibilities that everyone working with children has to safeguard their welfare.

Related Guidance

This guidance forms part of a wider range of child protection and safeguarding documents and the following in particular should also be referenced

- Education e safety Policy Guidance; Enfield Safeguarding Children Board
- Child Protection Guidelines for Childminders, Early Years Settings and Out of School Clubs
- Statutory Framework for the Early Years Foundation Stage 2014

Good Practice for Staff and Volunteers Photography and Videos

All Early Years Settings should register with the Information Commissioner’s Office as they process personal data where photography is used.
ICT has an important role in supporting children's learning and development. For example, photographs of children engaged in a variety of activities and experiences can provide valuable evidence to include within learning journals.
To promote safer use of ICT, it is essential that when work with children involves the taking or recording of images this should safeguard the privacy, dignity and well being of children. Informed written consent, using a proforma such as the attached, should be obtained from parents or carers and agreement should also be sought from the child, where possible.
Care should be taken to ensure that all parties understand the implications especially if the image is to be used for any publicity purposes or published in the media. There should be agreement as to how the images will be stored, and for how long.

Adults need to be sensitive to children who appear uncomfortable and be alert to the potential for such activities to lead to misunderstandings.
It is not appropriate for adults to take photographs of children for their own personal use.

Helpful Hints

Do

- Be clear about the purpose of the activity and what will happen to the images
- Be able to justify images of children in your possession
- Avoid making images in one to one situations or that show a single child with no surrounding context
- Ensure the child understands why the images are being taken and that they are appropriately dressed
- Only use equipment provided or authorised by the organisation
- Report any concerns about inappropriate or intrusive images found
- Ensure you have parental permission to take and/or display photographs

Do Not

- Display or distribute images without consent
- Use images that could cause distress
- Use personal mobile phones or other personal devices to take photographs, (unless you have specific authorisation)
- Take images ‘in secret’ or images in situations that could be construed as being secretive

Closed Circuit Television (CCTV)

Settings are increasingly using CCTV which can help in monitoring and security both within the setting and around the external site. This can be particularly helpful in buildings where there are corridors or areas out of sight. Settings using CCTV should observe the following

Do

- Ensure areas covered by CCTV are clearly signposted
- Ensure the manufacturer’s instructions and data protection guidelines are followed at all times. This should include appropriate storage and disposal of all recordings
- Recordings should be retained for a limited time period and no longer than their intended purpose. Generally this is no longer than 30 days.

Recordings should be erased before disposal including recordings taken outside of operational hours

- Regular auditing of stored images should be undertaken by the lead practitioner or manager

- Ensure sensitive positioning of cameras to avoid inadvertently taking inappropriate images. Cameras should not be pointed directly at toilet cubicles or other sensitive areas
- Where images recorded give cause for concern or involve criminal activity, the information should be referred to the relevant agency

Access to Inappropriate Images and Internet Use

Many settings now use internet enabled devices, including iPad educational apps and games, to enhance the learning experience of children or as online tools for staff to track and share achievement. For this reason, great care must be taken to ensure that safe and secure internet access, appropriate for both adults and children, is made available regardless of the size of the setting.

There are no circumstances that will justify adults possessing indecent images of children. Accessing, making and storing indecent images of children on the internet are illegal. Adults who are involved in this activity will be viewed as a threat to children and will be subject to a criminal investigation that if proven will result in them being barred from working with children.

- Adults should not use equipment belonging to the setting to access pornography, nor should personal equipment containing such images be brought into the workplace.
- Adults should ensure that children are not exposed to inappropriate images or web sites. Appropriate controls should be in place to prevent this, for example, through use of filters and personal passwords. In larger settings age appropriate content filtering must be in place across the setting, ensuring that staff and children receive different levels of filtered internet access in line with user requirements (e.g. Youtube at staff level but blocked to children)
- Childminders and smaller settings must ensure that parental controls are established on all internet enabled devices that children have access to, blocking or preventing access to any harmful, illegal or inappropriate content.

Where indecent images are found, this must be reported immediately via the manager (unless the manager is the subject of the concern) who will alert the Police and/or the Local Authority Designated Officer (LADO).
Adults who discover such images should not attempt to investigate the matter themselves as this could compromise an investigation

Do

- Have policies in place about internet use for example through an acceptable use agreement
- Follow guidance on the use of IT equipment
- Ensure that children are not exposed to unsuitable material online
- Ensure that any films, games or material shown to children and young people are age appropriate

Communication with Children through technology

Communication between children and adults should take place within clear and explicit professional boundaries. This includes the use of technology such as mobile phones, text messaging, websites etc. Adults should ensure that all communications are transparent and open to scrutiny. There is a need to be cautious to avoid any possible misinterpretation of motives or behaviour that could be interpreted as grooming. Adults should not therefore give personal contact details to children unless in exceptional circumstances the need to do so is agreed with managers and parents. E-mail communications should be professional in tone and content and e-mail systems should be used in accordance with the acceptable use agreed policy.

Do

- Have an agreement about permissible and acceptable modes of communication
- Only use equipment provided by the setting to communicate with parents/children
- Only make contact with children for professional reasons and follow acceptable use agreement

Do Not

- Give out personal contact details to children or young people
- Use internet or web based communication channels to send personal messages to a child or young person

Use of Social Networking Sites

Social networking sites (e.g. Facebook and Twitter) can be a useful advertising tool for early year's settings and can often be an effective way of engaging with parents. Due to the public nature of social networking and the inability to keep content truly private, great care must be taken in the management and use of such sites. Best practice guidance states that:

- Identifiable images of children should not be used on social networking sites.
- To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the setting's page.
- Ensure that privacy settings are set to maximum and checked regularly.
- For safeguarding purposes, photographs or videos of looked after children must not be shared on social networking sites.

Staff should ensure that their personal use of social media does not conflict with their professional role and be mindful of information they post online. Staff should observe confidentiality and not discuss issues relating to work on line or bring the setting into disrepute. Privacy settings should be set to block unauthorised access to the account and staff should avoid accepting children and parents as 'friends' as this can compromise professional boundaries.

Applications for recording children's progress

In recent years, a number of applications (apps) for mobile devices have been launched which are targeted specifically at Early Years Practitioners and settings. Many of these apps allow staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. Such tools have considerable benefits, including improved levels of engagement with parents and a reduction in paperwork, but careful consideration must be given to safeguarding and data security principles before using such tools.

- Personal staff mobile phones or devices (e.g. iPad or iPhone) should not be used for any apps which record and store children's personal details, attainment or photographs. Only setting issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft.

- Before purchasing or accessing any apps for staff or children's use, Providers/Managers must have a clear understanding of where and how children's data will be stored, including who has access to it and any safeguarding implications.
- Please note: The Provider/Manager is ultimately responsible for the security of any data or images held of children within the setting.

Data Protection
Data Protection means that all who hold personal data either on paper or electronically must keep it secure.

Personal data is defined as any data that enables an individual to be identified including names, contact details, and so on.

Any item that can hold information requires controls to be put in place to prevent it being damaged or stolen. This will include CDs, DVDs and memory sticks. Sensitive data, photographs and videos of children should not be stored on setting devices which leave the premises (e.g. laptops, mobile phones, iPads, USB Memory Sticks etc) unless encryption software is in place.

All staff should be aware of the settings guidance regarding storage, transmission and removal to ensure data is kept safe.

Responding to Concerns

Any concern in a child care setting should in the first instance be reported to the Manager or Lead Practitioner, (unless they are the subject of concern) in which case seek advice from the Local Authority Designated Officer

The Manager will consider whether the concern needs to be referred to The Police and/or Children's Social Care as a safeguarding incident. If the concern is about the behaviour of staff or volunteers then it should be reported to the Local Authority Designated Officer.

For further detail, please refer to your Child Protection Procedures

Childminders are themselves the lead practitioner so should seek advice direct from children's social care and/or ofsted

Ofsted also need to be notified as soon as reasonably practicable, but not later than 14 days after the event.

Appendix C: Additional Resources

- https://learning.nspcc.org.uk/safeguarding-child-protection/writing-a-safeguarding-policy-statement