
HOPE2FAMILIES SAFEGUARDING POLICY

Data Protection Officer

70 Long Commons Coleraine
Coleraine, BT52 1LH
07856201383
wildfireministrys@gmail.com

Table of contents:

<u>Guidance for photographing and filming:</u>	3
<u>Risks of sharing images online:</u>	4
<u>Seeking consent to share images of children and young people: When is consent needed?</u>	5
<u>How to get consent:</u>	5
<u>What to do if consent isn't given:</u>	6
<u>Storing images securely:</u>	6
<u>References and resources:</u>	8
<u>Childline:</u>	8
<u>Child protection records retention and storage guidelines</u>	9
<u>Summary</u>	16
<u>Contact details:</u>	17
<u>Find out more about:</u>	18

Guidance for photographing and filming:

It's important that children and young people feel happy with the photographs and films they appear in. Family and friends also want to be able to share the successes of their children when they have been part of a special event or activity.

However, some children, parents or carers may not be comfortable with images of themselves or their children being shared. For example:

- If a child and/or their family have experienced abuse they may worry about the perpetrator tracing them online
- Children who choose not to have contact with some members of their family may decide to minimise their online presence
- Families may have religious or cultural reasons for choosing not to be photographed

It's important to be aware of child protection and safeguarding issues when taking photos of or filming children and young people. The potential for misuse of images can be reduced if we are aware of the potential dangers and put appropriate measures in place.

We also consider the data protection implications of making, using and storing images of children and young people for your charity's use.

Risks of sharing images online:

Sharing photographs and images of children on social media or other online platforms carries potential risks. For example:

- Children may become vulnerable to grooming if a photograph is shared alongside information that makes them identifiable. This includes: personal details; a tag with location information; visual details such as a school uniform
- Inappropriate images of children may be shared online
- Images may be copied, downloaded, screenshotted or shared by anyone
- Images of children may be adapted and used inappropriately

- Photos or videos may appear in internet search results
- Depending on the terms and conditions of using an online platform, the image may be owned by the platform once it's been posted. Platforms may then licence images for use by third parties – such as for commercial purposes
- Each photo or video, and any comments on them, become a part of a child's public image. This may affect them later in life – for example, it may affect how they see themselves, or how they are viewed when applying for a job

(Thinkuknow, 2021).

Before sharing images of children on social media, we will consider how widely images may be shared, how long they may remain available and how this may affect the children's long-term wellbeing.

Seeking consent to share images of children and young people: When is consent needed?

Children will be consulted about the use of their image and give consent to it being used and shared.

For young people under 16, we will also get parental consent to use an image.

In situations where under 16s are separated from their parents (for example if they are in care) we will seek consent from someone who holds parental responsibility (for example the child's carer or the local authority).

For 16- to 17-year-olds, we will decide if it's appropriate to obtain parental consent, depending on the activity and the young person's circumstances. If we decide we do not need parental consent, then we will consider whether to inform parents that the child's photograph is being shared. In most circumstances, parents have a legal parental responsibility for their children up to the age of 18.

How to get consent:

We will make sure children, young people, their parents and carers understand what they are agreeing to.

- Make them aware that a photo or video is being taken.
- Explain what the image is going to be used for.
- Ask for their consent to share their image and record this on a written consent form.
- Tell them how long their consent is valid for and how long you will keep the image for.
- Explain what you will do if a child or their parents change their mind and withdraw consent at a later stage.
- Make it clear that if a child's image has been used online or in printed publications it will be very difficult to recall it if consent is withdrawn.

A record of the written consent that parents, carers and children have given for images being used.

It's good practice to share the photography policy we have with children and parents and seek their consent at the beginning of the year. We may also need to get additional consent in specific circumstances (if for instance, we are bringing in a professional photographer or the photos might appear in the local or national media).

What to do if consent isn't given:

If children and/or their parents and carers don't want to have their photo taken or shared, we will respect their wishes.

Children should never be excluded from an activity because we don't have consent to take their photograph.

In advance of a photography session we should agree with parents, carers and the child the best way for them to be identified so the photographer knows not to take photos of them. This might involve giving them a badge, sticker or wristband. Whichever method we choose, we should make sure children don't feel singled out or isolated.

Storing images securely:

If our charity stores images or video recordings of children for official use, we must ensure we are complying with the Data Protection Act 2018.

We must take steps to mitigate the risk of unauthorised access to and inappropriate use of images of children. This might include:

- Storing images in a secure location
- Encrypting electronic images before they are stored
- Only using devices belonging to our organisation to take and store photos and recordings of children
- Making sure anyone who takes or uses images of children for our charity has permission to do so.

In Hope2Families we work very closely with children, young people, their families and outside agencies and there is a possibility that we will come into contact with confidential or sensitive information.

Confidential information is information which is not lawfully in the public domain or readily available from another public source. In this organisation it is our intention to respect the privacy of children and young people and their parents. We aim to ensure that all parents can share information with us in the confidence that it will only be used to enhance the welfare of their child.

This charity will respect confidentiality in the following ways:

- Parents will have ready access to the records of their own child/children, but will not have access to information about any other child;
- Information given by parents to staff and volunteers will not be passed on to other adults without permission, except with regard to a safeguarding concern;
- We inform parents when we need to record confidential information beyond the general personal information we keep – for example with regard to any injuries, concerns or changes in relation to the child or family, or any discussions with parents/carers on sensitive matters;
- We keep all records securely.

Signed: Date:

Review date:

References and resources:

Ask the Police (2021) Q717: I want to take some photos / video footage in public, is it now illegal? [Accessed 09/12/2021].

Department for Education (DfE) (2018) Data protection: toolkit for schools. London: DfE.

Information Commissioner's Office (ICO) (2017) In the picture: a data protection code of practice for surveillance cameras and personal information (PDF). [Wilmslow]: ICO.

Information Commissioner's Office (ICO) (2021a) Guide to data protection. [Accessed 28/07/2021].

Information Commissioner's Office (ICO) (2021b) Data storage. [Accessed [Accessed 28/07/2021].

Information Commissioner's Office (ICO) (2019c) CCTV checklist. [Accessed 28/07/2021].

Ofsted (2019) Surveillance and monitoring in residential childcare settings: information for providers and managers on the use of surveillance, including CCTV, in their residential childcare settings and how Ofsted will evaluate its use. [Accessed 28/07/2021].

Thinkuknow (2021). Sharing pictures of your children online. London: National Crime Agency's CEOP Command. [Accessed 28/07/2021].

Childline:

If a child or young person needs confidential help and advice after an image of them has been shared online, direct them to Childline. Calls to 0800 1111 are free and children can also contact Childline online. They can get advice from the website about:

- Online and mobile safety
- Reporting a nude image online and requesting removal

Child protection records retention and storage guidelines:

If an organisation needs to hold records about a child or adult for any reason, it must have policies and procedures in place regarding the retention and storage of that information.

Our charity must:

- Know the reason why you're keeping records about children and/or adults (for example, because they relate to child protection concerns)
- Assess how long you need to keep the records for
- Have a plan for how and when the records will be destroyed

To keep personal information secure, you should:

- Compile and label files carefully
- Keep files containing sensitive or confidential data secure and allow access on a 'need to know' basis
- Keep a log so you can see who has accessed the confidential files, when, and the titles of the files they have used. If we are creating records about the children and/or adults that take part in your services or activities, we need to make sure they understand what records we hold, why we need to hold them and who you might share their information with (for example as part of a multi-agency child protection team) (Information Commissioner's Office, 2021). If we are keeping records for child protection reasons, we don't necessarily need to get consent from the adults and/or children concerned

We must keep an accurate record of:

- 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 report
- 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 our charity decided not to refer those concerns to a statutory agency (if relevant). We will 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. We have created a standard form for recording concerns. This ensures all the necessary information is collected consistently

How we keep our records:

Electronic files should be password protected and stored on computers with protection against hackers and viruses.

- Information about child protection concerns and referrals should be kept in a separate child protection file for each child, rather than in one 'concern log'. The child protection file will be started as soon as we become aware of any concerns.
- It's good practice to keep child protection files separate from a child's general records. We will mark the general record to indicate that there is a separate child protection file.
- If we need to share records (within your own charity or externally), we will make sure they are kept confidential. Use passwords and encryption when sharing electronic files.

- If our staff and volunteers use their personal computers to make and store records, we need a clear agreement to ensure the records are being stored securely.
- If the person responsible for managing our child protection records leaves our charity, we will make sure we appoint somebody to take over their role and arrange a proper handover.

Recording concerns about adult behaviour:

- Sometimes concerns might be raised about an adult who works or volunteers with children. This could be because they've:
 - Behaved in a way that has harmed, or may have harmed, a child
 - Committed a criminal offence against, or related to, a child
 - Behaved in a way that indicated they are unsuitable to work with young people

In response to future requests for a reference:

- If a future employer asks for clarification about information disclosed as part of a vetting and barring check
- If allegations resurface after a period of time.

Storing records relating to adults:

Records relating to concerns about an adult's behaviour should be kept in the person's confidential personnel file (not in a central 'concerns log') and a copy should be given to the individual.

Retention periods: concerns about adults:

If concerns have been raised about an adult's behaviour around children, the general rule is that we should keep the records in their personnel file at least until they reach their normal retirement age or for 10 years – whichever is longer (IRMS, 2019; Department for Education, 2021). This applies to volunteers and paid staff.

For example:

- if someone is 60 when the investigation into the allegation is concluded, keep the records until their 70th birthday
- if someone is 30 when the investigation into the allegation is concluded, keep the records until they are aged 65.

We will keep records for the same amount of time regardless of whether the allegations were unfounded. However, if we find that allegations are malicious we should destroy the record immediately

We must keep clear and comprehensive records of all allegations made against adults working or volunteering with children, including:

- What the allegations were
- How the allegations were followed up
- How things were resolved
- Any action taken
- Decisions reached about the person's suitability to work with children.

Keeping these records will enable us to give accurate information if we are ever asked for it.

When to share information:

Timely information sharing is key to safeguarding and promoting the welfare of children.

People who work with children, whether in a paid or voluntary role, may need to share information about the children and families they are involved with for a number of reasons. These include:

- We are making a referral to arrange additional support for someone in the family
- Someone from another agency has asked for information about a child or family
- Someone in the family has asked to be referred for further help
- A statutory duty or court order requires information to be shared
- We are concerned that a child or a member of their family may be at risk of significant harm
- We think a serious crime may have been committed or is about to be committed which involves someone in the family

We must always have a clear and legitimate purpose for sharing a child's personal information. Keep a record of the reasons why we are sharing or requesting information about a child or their family.

We should also make sure you are not putting a child's safety and welfare at risk by sharing information about them.

Some professionals have a legal duty to share information relating to safeguarding concerns. More information about this is available in the mandatory reporting tab.

We always seek consent to share information about a child and their family. However, if consent isn't given, we can still share information with relevant professionals under certain circumstances, for example if we are protecting a child from significant harm. The Data Protection Act 2018 and General Data Protection Regulation (GDPR) do not affect this principle.

What information to share:

We need to decide what specific information is appropriate to share and who to share it with.

- Prioritise the safety and welfare of the child and anyone else who may be affected by the situation
- Make sure we share the information quickly and securely. The sooner we report our concerns the better. This means the details will be fresh in our mind and action can be taken quickly
- Identify how much information should be shared. This will depend on the reasons for sharing it
- Use language that is clear and precise. Different agencies may use and understand terminology differently
- Make sure the information we are sharing is accurate. Make it clear what information is factual and what is based on opinion (yours or other people's)

Getting Consent:

It's important that children and families understand the reasons why we might need to share information to help keep children safe.

We should always seek consent to share information and it's important to get consent in writing.

What to do when wanting to see personal information: link below:

<https://www.nspcc.org.uk/globalassets/documents/terms-and-conditions/accessing-your-personal-information>

Summary:

As an organisation using AccessNI to help assess the suitability of applicants for positions of trust, Hope2Families complies fully with AccessNI's Service Level Agreement regarding the correct handling, use, storage retention and disposal of Disclosure Applications and Disclosure information. We also comply fully with obligations under the Data Protection Act 2018 and other relevant legislative requirements with regards to the safe handling, storage, retention and disposal of Disclosure Information.

Consent

As we no longer receive a copy certificate from AccessNI, written consent will be obtained from the Applicant when requesting and retaining a (copy of a) Disclosure certificate.

Storage and Access

Disclosure information is to be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Handling

In accordance with section 124 of the Police Act 1997, Disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Disclosures or Disclosure information has been revealed. We recognise it is a criminal offence to pass this information to anyone who is not entitled to receive it.

Usage

Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Retention

Once a recruitment (or other relevant appointment, regulatory or licensing) decision has been taken, we do not keep Disclosure information for any longer than is necessary. We comply with AccessNI's Service Level Agreement to return the original Disclosure certificate to the applicant once a decision, recruitment or otherwise has been made and will be retained no longer than the agreed period.

Disposal

Once the retention period has elapsed, we will ensure that any Disclosure information is immediately destroyed by secure means i.e. by shredding, pulping or burning. While awaiting destruction, Disclosure information will not be kept in any unsecured receptacle (eg waste-bin or confidential sack). We will not keep any photocopy or other image of the Disclosure or any copy or representation of the contents of a Disclosure or any other relevant non-conviction information supplied by police. However, despite the above, we may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the AccessNI unique reference number of the Disclosure Certificate and the details of the recruitment decision.

Contact details:**Contact details:****Nominated child protection lead:**

Marc Taylor

07514993163**wildfireministrys@gmail.com****Deputy child protection lead:**

Heather Taylor

07856201383**wildfireministrys@gmail.com****NSPCC Helpline****0808 800 5000****We are committed to reviewing our policy and good practice annually.****This policy was last reviewed on:**..... **24th May 2022**(date)**Signed:** *Marc Taylor****[this will be signed by the most senior person with responsibility for safeguarding in our charity, for example the safeguarding lead on our board of trustees].***

Find out more about:

<https://learning.nspcc.org.uk/safeguarding-child-protection/children-from-black-asian-minoritised-ethnic-communities>

<https://learning.nspcc.org.uk/safeguarding-child-protection/deaf-and-disabled-children>

<https://learning.nspcc.org.uk/safeguarding-child-protection/lgbtq-children-young-people>

<https://learning.nspcc.org.uk/safeguarding-child-protection-schools/safeguarding-children-with-special-educational-needs-and-disabilities-send>