Policy and Practice Guidance on Social Media and Internet Checks of Applicant Adopters

Document Title	Policy and Practice Guidance on Social Media and Internet Checks of Applicant Adopters
Version	1.2
Author/s	Nik Flavell, Senior Manager for Adopt North East and Emma Phillips, Information Officer
Owner	Nik Flavell, Senior Manager for Adopt North East
Date Approved	27/06/2023
Date to be Reviewed By	2/06/2025

The Purpose

The Adoption Agencies Regulations 2005 (as amended) do not specifically require social media and internet checks to be undertaken by the Agency. However, Regulations 25(5) and 30(f) permit the Agency to include 'any other information which the agency considers to be relevant'.

The Agency acknowledges that many applicants will have an online profile and participate in social networking. It is the policy of Adopt North East that it will undertake social media and internet checks as part of Stage 1 of the Adoption Process (References and Checks). It does do for two reasons:

i. A check by the Agency is undertaken to establish whether social media and internet use by applicant is such that it could enable an enquirer[1] to obtain from publicly accessible information personal information about the applicant which could potentially lead to the enquirer establishing the location of an adopted child;

ii. A check by the Agency is undertaken to establish whether social media and internet use by applicant reveals, from publicly accessible information, information that is relevant to informing a safeguarding understanding of the suitability of an applicant to care for a child.

The agency has a responsibility to ensure that the children and young people in its care are safeguarded from potential harm. This policy seeks to protect the interests of

[1] The Agency uses the 'Motivated Intruder Test' recommended by the Information Commissioner's Officer – a Motivated Intruder is 'a person who starts without any prior knowledge but wishes to identify an individual from whose personal data the anonymous information is derived' and tries to do so without recourse to specialist knowledge (eg in-depth knowledge of computer hacking), access to specialist equipment; or the need to resort to criminal acts to gain access to data that is held securely'. For more information see https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf

applicants, children, and the Agency. Accordingly, such checks are considered reasonable, proportionate and relevant.

Informed Consent

The Agency will only carry out a Social Media and Internet Check with the written consent of the applicant to do so. This consent will be sought at the Registration of Interest Stage.

The Agency will ensure that all applicants are informed of the purpose of the checks (as noted above) and what actions the Agency will take. This Guidance (and any future iteration) will be made publicly available on the Adopt North East website.

In the spirit of openness, the findings of the check will be shared in full by the Agency with the applicant unless to do so would place a child at risk of harm.

The Process – Internet Check

An 'internet check' by Adopt North East will be carried out by the applicant's allocated Social Worker during Stage 1. This will involve the Social Worker putting in the applicant's name/s using a reputable, commonly used and publicly available search engine and viewing any publicly available (open source) linked sites.

The Agency will not seek access to password protected sites as this information is not within the public domain. Any findings will be shared with the applicants by their allocated Social Worker unless to do so would place a child at risk of harm.

All applicants will be advised by the Agency from the point of Registration of Interest about the need to maintain appropriate confidentiality throughout their adoption journey.

The Process – Social Media Check

Given the diversity and changing nature of Social Media platforms in use, the Agency will ask applicants to identify their 'primary' platform (the one they consider to be their current, main social media account and/or the one that has the most self-generated content) at the Registration of Interest stage.

It is not possible to give a definitive list of the platforms that may be searched by the Agency due to the constantly changing popularity of such platforms. This 'primary' platform will be subject to a check by the Agency.

Social Media checks by Adopt North East will be carried out by the applicant's allocated Social Worker during the course of Stage 1 of the Adoption Process (References and Checks). This will involve the Social Worker putting in the applicant's social media account name/s to its own account and viewing any publicly available (open source) information.

Any findings will be shared with the applicants by their allocated Social Worker unless to do so would place a child at risk of harm.

All applicants will be advised by the Agency from the point of Registration of Interest about the need to maintain appropriate confidentiality throughout their adoption journey.

Important Restrictions on Social Media and Internet Checks by Adopt North East

a) The Agency will not set up or use a false identity for the purposes of a Social Media check.
b) The Agency will use an identifiable social media account for the purposes of a Social Media check. This account will not be disclosed by virtue of the check being undertaken. Applicants will not be asked to allow the Agency or a member of Agency staff to join their public or private Social Media account/s.
c) Individual Staff Members will not use their personal social media accounts to undertake any checks on behalf of Adopt North East.
d) Individual Staff Members will not ask to view the personal social media accounts of applicants.
e) The Agency will only undertake a single internet check (once only) relating to an applicant, using a reputable, commonly used and publicly available search engine.
f) The Agency will only undertake a single check (once only) of a social media platform, although it may check multiple platforms once given the diversity of commonly used platforms.
g) Even though the Agency may have the consent of the applicant to undertake more than one check of the internet or social media, the Agency will not do so as such practice would likely constitute a breach the Regulation of Investigatory Powers Act 2000.

Considerations and Actions by the Agency following a check

The Agency will need to consider the information obtained during the check.

In the spirit of openness, the findings of the check will be shared in full by the Agency with the applicant unless to do so would place a child at risk of harm.

The Agency may advise the applicant that the check raised no issues of concern. The Agency may recommend changes that may be appropriate, for example, changes to privacy settings to reduce the amount of information in the public domain. The Agency may advise that information within the public domain may raises a concern that will be addressed further in assessment or, exceptionally, that information raises significant concern about the suitability of the applicant to adopt.

The feedback of the Agency will be dependent upon the Internet or Social Media check.

Issues that may raise concerns are listed below. The list is non-exhaustive but is intended to be indicative of the sorts of issues that will be considered by the Agency:

- Photographs, videos, posts, messages or any other content that is, in the judgment of the Agency offensive or may reasonably be said by the Agency to be likely to cause offence;
- Likes, Sharing or other affirmation of content that are, in the judgment of the Agency offensive or may reasonably be said by the Agency to be likely to cause offence;
- Membership of Social Media Groups that are, in the judgment of the Agency inimical to the values required of adopters
- Content that contradicts information provided by the applicant relevant to assessment, for example pictures of the use of alcohol by the applicant when the applicant has stated that they do not use alcohol; messages to an individual that they have stated they have not contact with; evidence of a previous adoption application which has not been reported to the Agency etc.
- Content that evidences a potential lack of openness and honesty with the Agency relevant to assessment, for example evidence of additional employment, property or relationships, etc.
- Content that evidences an actual or potential risk by the applicant to children or others

The Agency notes that consideration will be given as to the distinction between content of concern generated by the applicant and content received by the applicant by but generated by someone else.

<u>The Agency will advise of the following Good Practice for Applicant Adopters</u>

Applicants should, upon Registration of Interest that they are interested in adopting:

- Check their security and confidentiality settings and change them where necessary to ‘private’;
- Refrain from posting, messaging or referring to their adoption journey on any publicly available (Open source) platform;
- Consider whether any historical content is likely to be an issue and let the Agency know
- Consider all future generated content and its appropriateness in light of their adoption journey
- Apply the ‘motivated intruder’ test to content – assume that your content will be scrutinised by determined person with a particular reason to want to identify individuals
- Ensure absolute confidentiality in any matters relating to children in care disclosed by the Agency as part of the adoption process

<u>Legal Considerations</u>

The Human Rights Act 1998 gives a ‘right to respect for private and family life, home and correspondence’. The provision is directly enforceable against public sector

employers, and all courts must interpret other existing legislation in relation to the Human Rights Act.

The Regulation of Investigatory Powers Act 2000 (RIPA) governs the use of covert surveillance by public bodies.

The Data Protection Act 2018 is the UK's implementation of the **General Data Protection Regulation** (GDPR) the act controls how your personal information is used by organisations, businesses, or the government.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage