E-SAFETY AND YOUNG PEOPLE

Improving understanding and support in the social housing sector
CONTENTS

Background 3
Research focus and key findings 4
Why should e-safety be important to social housing providers? 6
Why focus on young people? 7
Progressing e-safety in the social housing sector 8

Appendices 9
Appendix 1 9
Appendix 2 11
Orbit Group owns and manages 39,000 homes and has around 100,000 customers. We work in the Midlands, the East and South East regions, and parts of London through our housing associations: Orbit Heart of England, Orbit East and Orbit South. We don’t just provide general needs homes, but also serve some of the most vulnerable people in the community.

Our digital inclusion programme has been developing since 2013, with significant investment in helping our customers get online through communal wifi projects and individual grants, and supporting digital skills development through partnerships with a wide range of national and local organisations.

Through our focus on digital inclusion, we began to identify potential gaps in awareness and knowledge about e-safety issues, particularly amongst young people that we work with. Being safe online is fast becoming a life skill and one that is essential for everyone to ensure that we can all socialise, work and shop safely in the online as much as in the offline world.

Findings for 2014 from the Office of National Statistics reported that 76% of people in the UK are online, with young people (aged 16 to 24) most likely to use social media (91% of young people online). With the rising use of social media there is an increasing urgency to ensure that everyone who is online is able to use the internet safely and responsibly. Research for the BBC found that over half of children aged 11 to 16 surveyed had done something risky or anti-social online.

Orbit takes the safety and wellbeing of our customers and their families seriously. Against the backdrop of national research and local experiences of our staff and customers we commissioned Charlotte Aynsley, e-Safety Training and Consultancy, to investigate the reality of the risks that our customers, especially young adults, face and to advise the organisation on what we can do to improve awareness and support.

The key findings from the research, completed early in 2015, are below. We believe that these findings and recommendations are relevant to the social housing sector as a whole and we welcome partnerships and collaboration to take forward this important issue.
RESEARCH FOCUS AND KEY FINDINGS

The focus of the research commissioned by Orbit included:

1. Understanding the type of e-safety risks that young people face and the extent to which they may be exposed to or they may undertake online activities that pose potential risks to themselves and others.

2. Understanding the perspective of Orbit staff and community partners in terms of the e-safety related issues they have encountered when supporting young people and how confident staff and partners feel in helping young people deal with online risks and issues.

3. Exploring ways to provide effective support, advice and information to young people and staff members to improve understanding of e-safety risks and how to deal with them when encountered.
RESEARCH FOCUS AND KEY FINDINGS

Evidence was gathered through:

- An online survey which received 60 responses (split approx. 50/50 between young people aged 24 and below and people aged 25+). This split provided a useful comparison between behaviours and attitudes towards e-safety amongst young people and older age groups.

- An online survey targeted at Orbit staff and community partners.

- A workshop held with Orbit staff working in front-line teams.

- Discussions with young people and staff at a local youth organisation and at several supported schemes managed by Orbit.

- A review of Orbit’s Safeguarding and Child Protection policies to identify opportunities to integrate e-safety.

- Discussions with Community UK.net Ltd, our main customer-facing wifi provider, regarding management of internet access.

The feedback, experiences and ideas gathered through these activities has provided a good basis for improving our understanding of key online behaviours, potential areas of risk and options to explore to improve engagement with young people. Key findings included the following:

- Young people rely mostly on their smart phones (a personal/private device) for access to the internet and for accessing social media apps and websites. They are also more likely to share content they generate (such as messages and photos) than other age groups.

- Young people feel safer online than other age groups, but may be more regularly exposed to e-safety risks. This higher confidence may suggest that they are better able to deal with online risks, however our discussions with young people and their low awareness of expert sources of e-safety advice suggests that in reality they may underestimate risks and may not be aware of how some of the content they share online may be used.

- Staff members and community partners do see themselves as having a role to play in helping young people stay safe online as part of their wider professional roles. Staff members also highlighted many areas where e-safety risks or incidents were related to wider issues around customers’ vulnerabilities or disputes with others.

- The ‘digital footprint’ that young people generate and share online is an increasingly important factor in how others, such as potential employers, perceive them. This can be positive or negative, so it is important that young people understand their digital footprint.
WHY SHOULD E-SAFETY BE IMPORTANT TO SOCIAL HOUSING PROVIDERS?

On the surface, the high uptake and use of online services amongst young people suggests that they are least in need of digital inclusion support. Rightly, our focus on helping people get online focuses predominantly on older people as the group with lowest internet use. However, e-safety does have important links into wider priority areas:

- **Employability**: internet access and digital skills are now integral to improving employment and training outcomes. In parallel with this, our online behaviour and our ‘digital footprint’ (information shared online that continues to be available long after it may have been expected to) is also becoming a more significant factor, both positively (for example by being able to showcase skills and achievements to prospective employers) and negatively (through an online profile that shows inappropriate behaviour and poor judgement).

- **Financial inclusion**: sharing information about ourselves online and engaging with large networks of virtual ‘friends’ can lead to greater exposure to scams, fraud and identity theft. This could be through sharing personal information that is valuable to fraudsters or through being more trusting of contacts that are online only. Critical thinking skills are important for evaluating the accuracy and trustworthiness of information offered on websites, social media and other online channels.

- **Wellbeing**: the evidence around the impacts on mental and emotional wellbeing of cyberbullying and victimisation are clear. The effects of online sexual exploitation are also well known; it should also be noted that sexual exploitation is not limited to predatory grooming – there is also growing evidence that many young people are sharing explicit images of themselves which could be used by others to blackmail or bully individuals.

Given that for many young people, as for many other age groups, online life is not separate to ‘real’ life, it is important that support services include consideration of e-safety to the same degree as addressing physical risks and issues that our customers may face. By excluding e-safety considerations, we risk missing an important and growing part of many people’s lives in the advice, support and guidance we offer.

Many housing associations and third sector partners also work with and support vulnerable young people. It is important that e-safety forms part of wider advice and support provided to vulnerable groups and that the added risks that vulnerable individuals may be exposed to online are understood and considered.
WHY FOCUS ON YOUNG PEOPLE?

It is generally assumed that teenagers and young adults are ‘internet savvy’ and are often characterised as ‘digital natives’ due to having grown up using digital and online technologies. Recent years have also seen internet safety education rising in profile (see Appendix 1), with schools expected to address e-safety within the curriculum and with many campaigns aimed at parents and children/teenagers.

Our initial discussions with staff and customers prior to commissioning further research suggested the following:

• Young people are both highly likely to be online and very frequently share information about themselves and others via photos, messages and other content.

• Young people may be more likely to engage in potentially risky behaviour online such as sharing personal information and photos and may also be more likely to be targeted by others online.

• Whilst there may be a higher general awareness of e-safety, young people may lack the knowledge to know how to deal with specific issues and where to turn to for help.

Some young customers may also have limited understanding of their digital footprint. This can have impacts such as:

• Negatively affecting employment prospects where information about anti-social or where disreputable activities are associated with their online profile.

• Sharing information about their children which may continue to affect those children when they reach adulthood (such as photos or videos that the child may find embarrassing or compromising).

Prior to undertaking our research with Orbit customers and staff, we found that there are good e-safety materials already available, but that these are aimed largely at two audiences: parents and children or older people. We found fewer resources that are aimed specifically at young adults, or that can successfully engage those for whom current e-safety education has not worked. Examples of e-safety resources and related research are provided in Appendix 2.
Many organisations provide online safety advice to their customers as part of their broader duty of care and where they have a legal responsibility, such as in schools and colleges. It could be argued that, where social housing organisations provide care and support to potentially vulnerable young people, e-safety advice is crucial especially if they are under 18.

Appendix 1 outlines the policy and practice framework used by schools and colleges for e-safety. The ‘PIES’ model in Appendix 1 could be applied to the social housing context and would provide a helpful way to help to mitigate risks in the online context.

Orbit is taking forward key actions to improve our support:

- We are integrating e-safety into our wider safeguarding policies and staff training provision. We will also identify key touchpoints where we can promote e-safety, for example as part of employability advice and support.

- We are working in partnership with Childnet International to build on their expertise and guidance to improve awareness amongst our customers, community partners and staff members.

- We are continually reviewing where we have opportunities to promote e-safety, for example through improving guidance available via shared wifi login processes, via our website and through our customer magazine.

- We will be supporting Safer Internet Day 2016 (9 February) and joining this national campaign to improve awareness of e-safety.

We believe all social housing providers have an important role to play in understanding how e-safety affects their customers and how individual organisations and the sector as a whole can help everyone stay safe online.
Recognising and addressing the risks and impacts of online abuse, cyberbullying and other negative effects on young people is not new. e-Safety is now well established as part of wider safeguarding and inspection frameworks in sectors such as formal education. An overview of established approaches used to mitigate risks is provided below.

The potential risks

The risks posed online are often characterised using the following framework developed through the Government commissioned Bryon Review ‘Safer Children in a Digital World’ (2008):

<table>
<thead>
<tr>
<th>Content (Child as recipient)</th>
<th>Commercial</th>
<th>Aggressive</th>
<th>Sexual</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adverts</td>
<td></td>
<td>Violent/hateful content</td>
<td></td>
<td>Bias</td>
</tr>
<tr>
<td>Spam</td>
<td></td>
<td></td>
<td></td>
<td>Racist</td>
</tr>
<tr>
<td>Sponsorship</td>
<td></td>
<td></td>
<td></td>
<td>Misleading info</td>
</tr>
<tr>
<td>Personal info</td>
<td></td>
<td></td>
<td></td>
<td>or advice</td>
</tr>
<tr>
<td>Violent/hateful content</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pornographic or unwelcome sexual content</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bias Racist Misleading info or advice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Being bullied, harassed or stalked</td>
<td>Meeting strangers</td>
<td>Being groomed</td>
<td>Self-harm Unwelcome persuasions</td>
<td></td>
</tr>
<tr>
<td>Meeting strangers</td>
<td>Being groomed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tracing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harvesting personal info</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tracking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harvesting personal info</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tracking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harvesting personal info</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-harm Unwelcome persuasions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illegal downloading</td>
<td>Bullying or harassing another</td>
<td>Creating and uploading inappropriate material</td>
<td>Providing misleading info/advice</td>
<td></td>
</tr>
<tr>
<td>Hacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gambling</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial scams</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terrorism</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Providing misleading info/advice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

These risks vary depending on types and levels of access, levels of vulnerability and levels of education and protection in place. As all of these evolve, the risks in some areas intensify. For example high levels of access to smartphones can lead people to create and upload inappropriate sexual material as illustrated by the Child Exploitation and Online Protection Centre’s (CEOP) ‘Exposed’ film. Importantly, the Content/Contact/Conduct framework acknowledges that children (or young people and adults) can be actively involved in taking risks online or negatively impacting others through their online behaviour.

In order to mitigate e-safety risks, they first need to be understood and then mitigations put in place to manage them. They will, as highlighted above, evolve over time so they will need ongoing review.
Online safety in other contexts
Many organisations, both private and public, provide online safety advice support and information for their customers (see Appendix 2 for examples). Some social networks that target children are especially proactive in providing advice to children and their parents through targeted advice, support and information and help with reporting and escalation. This is usually provided at timely moments and point of sign up – see Disney’s Club Penguin as an example.

Where organisations including schools and colleges have more formal responsibility for children and young adults, their level of support can be more direct. They often follow a risk mitigation approach (The PIES model) that has been developed to guide e-safety approaches for schools and colleges in the UK.

This model helps to mitigate risks through organisations having the right kind of policies and practices in place, a safe and secure infrastructure, good levels of education and training for all stakeholders and all of this underpinned by a process of monitoring and review (standards and inspection). Educational institutions that provide access to technology especially for children use this model as the basis for mitigating risks to children and young people.
APPENDIX 2: EXAMPLES OF E-SAFETY MATERIALS AND SOURCES OF SUPPORT

Examples of resources promoting e-safety
Childnet International: resources for young people, parents and professionals
Canadian Schools Network: Kids Read Mean Tweets
UK Government: Cyberstreetwise
Microsoft YouthSpark Hub
Well Versed
ChildLine: Zip It

Social media guides
NSPCC: Share Aware and Net Aware
UK Safer Internet Centre Social networks guidance
Snapchat safety centre
Facebook Safety Centre
Instagram Safety Centre
Twitter Safety Centre
YouTube Safety Centre

Sources of expert knowledge and reporting tools
Child Exploitation and Online Protection Centre (CEOP): Safety centre
Internet Watch Foundation
Safer Internet Centre

Research and evidence
BBC Learning: BBC Be Smart 2015 audience survey
Internet Watch Foundation: Emerging Patterns and Trends Report #1: Youth-Produced Sexual Content

Related analysis by Microsoft:
New data on youth ‘nudes’ show highly disturbing trend
Experts: Don’t blame the victims of youth ‘selfies’