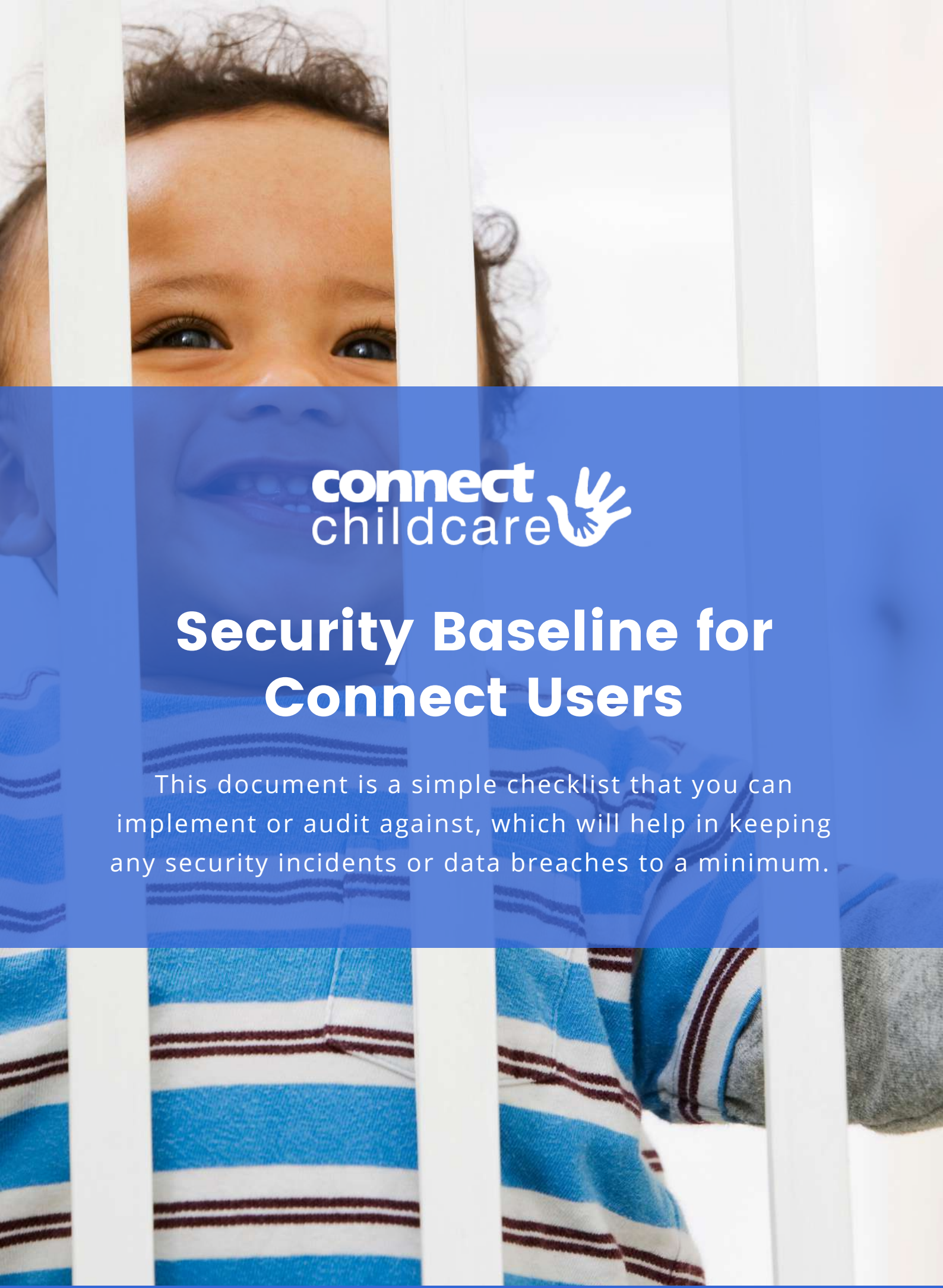


connect childcare

Security Baseline for Connect Users

This document is a simple checklist that you can implement or audit against, which will help in keeping any security incidents or data breaches to a minimum.

Security Baseline for Connect Users

In a world of increasing cyber threats, in quantity, complexity and variety, the role of security within IT is more important than ever. As a key provider of childcare software, we at Connect Software Solutions, are committed to ensuring that all child data is protected against unauthorised disclosure or modification.

As your business will be connecting to our infrastructure, we have a duty to ensure that all systems are as secure as possible. In addition to this, the implementation of new data protection legislation (such as the GDPR and Data Protection Act 2018) has mandated the consideration of security when handling any personal data. This is especially important with child data due to the stricter controls the new legislation has bought forward.

This document is a simple checklist that you can implement or audit against, which will help in keeping security incidents or data breaches, from both sides to a minimum.

CHECKLIST

1 Ensure your systems and data is stored in a physically secure area

If you are using hardware such as laptops, PC's, tablets or even server infrastructure, ensure you are keeping these in a secure physical location. Laptops and PC's can be physically secured using devices such as Kensington locks. Also, ensure your IT room is physically secure using locks and strong doors and managing who has access to it.

2 All endpoints and servers that deal with data have Anti-Virus running

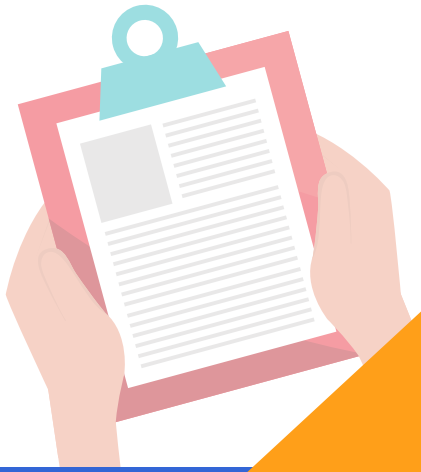
Anti-Virus software is usually the last line of defence for your asset against malware/viruses so ensure that you are using one. Although they are not 100% foolproof, they can prevent the more common malware/viruses from entering. There is a number of reputable AV software available, both paid and free, that will work depending on your needs.

3 All assets are accounted for and tracked

One of the biggest reasons data breaches occur is due to untracked assets (e.g. laptops, tablets, USBs) with personal data stored on them. Therefore, it is an essential task that your business tracks these assets and they are reported lost/stolen as soon as possible so that remediation actions can be completed.

4 A clear policy on usage of removable media in respect to data

Following on from the previous point, one way you can completely avoid this is to forbid any storing of data on removable media such as USBs. Also, you may want to consider implementing a policy on what data can be stored on a laptop / PC hard drive (e.g. no personal data allowed).



CHECKLIST

5 Patching policy in place for all servers, tablets, systems and endpoints

Some of the common attacks used by cybercriminals are via unpatched systems such as unpatched laptops, tablets and servers. Patches usually contain fixes to security vulnerabilities that may be used by cybercriminals. It may be worth scheduling a 'patching day' with your IT team, where you bring systems down for a set time to update software or the operating systems e.g. Windows updates.

6 Encryption policy in place for all systems

If you require personal data stored in a physical location such as on laptops or servers, it may be worth encrypting the data held within to prevent unauthorised disclosure or modification. If a laptop with personal data goes missing and the laptop hard drive was encrypted, criminals will be unable to access the data without the encryption key.

7 Firewalls in place (whether soft or hard) on key assets

Firewalls can come either software or hardware-based but they essentially function the same way. They control network access to devices or servers with a configured set of rules. They are key components when securing any system. If you do not employ any firewalls, strongly consider using one (either soft or hard) and ensure you are consistently reviewing the rules on it. Speak to your IT team if you are unsure about this.

8 Security incident management/data breach management in place

Security incidents/data breaches are unfortunate occurrences but if managed properly, can provide essential information. Not only are they key requirements in data protection legislation, but they can also help pinpoint gaps where security can be weak.

CHECKLIST

9 All staff are adequately trained regarding security/data protection

The biggest weakness in any system is always human error, whether that be as a result of misconfiguration of systems or a staff member being duped by a phishing email. The training of your staff can reduce security incidents/data breaches dramatically. There are a number of free resources available online that can be leveraged for this.

10 Implement policies around account/password management

All accounts, especially with access to child data, should be assigned to a single user only. This is so that any actions completed by an account is tracked to a single user. If the account is being shared between people, it becomes difficult to track who is changing what. On a related note, ensure you are constantly reviewing which accounts are being used and if a staff member leaves your business, ensure that their account is removed or disabled.

Further Considerations

The above checklist is intended to be as simple as possible, securing data as efficiently as possible without too much effect on your business. However, they do not cover all areas and there is a breadth of information available on further fine-tuning of any system if you wish to protect your system further.

Consider implementing further security actions such as certifications and external auditing as they can help further fine-tune your infrastructure.

connect childcare

We develop management software that improves the lives of children, globally. Through our software solutions, nurseries are becoming more efficient, enabling them to spend more time developing the children in their care. We are passionate about child development and support our customers to provide the very best quality childcare.

WWW.CONNECTCHILDCARE.COM

@CONNECTCHILDCARE

/COMPANY/CONNECT-CHILDCARE

@CONNECT_GROUP