Thrive
Acceptable Use Policy

Introduction
Thrive is a secure location to place and communicate confidential information where privacy is vital. Confidential information includes all information relating to county business. If you are in doubt as to what information may be disclosed, you should check with your line manager.

This Acceptable Use Policy (AUP) sets out a few basic principles for your use of the Thrive system and the information that it holds.

You will be made aware of any changes to this policy as they occur.

Registration
You will only be given access to Thrive after your identity and authority have been verified, a DBS check has been conducted and you have confirmed your understanding and abidance to this Acceptable Use Policy. Your DBS should be renewed every three years.

Basic Principles
Thrive is provided solely for the purpose of communicating your work documents in a secure environment. It is not to be used to comment on personal interests you may have outside of your professional interests and your working life. Kent County Council (KCC) values trust and responsibility in all relationships, and expects you to exercise personal responsibility when you place documents on Thrive.

If you are reported as having breached the AUP, this may result in disciplinary action and could result in termination of employment. KCC reserves the right to report any illegal or criminal violations to the appropriate authorities.

Where the administrator receives a complaint about a particular piece of information, they have the final say in deciding whether it should be removed or edited. The administrator reserves the right to remove any information without warning.

Do:

- be particularly careful to secure access to the network by using your password when working away from your office
- adopt a responsible approach to the content of documents you place on Thrive
- respect copyright and/or intellectual property rights. If you reproduce material from elsewhere then you must reference the source
- log out of Thrive and invoke the PC’s screen-saver/lock-out mechanism if you are leaving your computer unattended
- always log out of Thrive and close the browser page when you have finished using the system

Do Not:

- share your password with anyone – not even the Thrive administrator
- store KCC data on portable devices such as USB memory sticks, Laptops, Mobile Phones unless the device is fully encrypted as part of y our organisations security policy.
- store personal data on the system unless the storage is covered by KCC’s data protection registration under the Data Protection Act 1998
- allow members of your family or any unauthorised person to use the KCC network or KCC equipment
- display confidential information on the screen of your laptop at any time where it may be visible to others

- place on Thrive material that is defamatory or intended to offend, annoy, harass or intimidate another person or persons. This includes ethnic slurs, racist comments, personal insults, obscene/indecent words or suggestions; and be careful of sensitive topics such as politics or religion
- entice or encourage other users to post such material either, or respond to comments or posts in a way that may provoke aggressive responses
- place on the Thrive material that gives strong personal or political opinions, which may be misconstrued as being representative of your employer’s policy or strategy

Your Responsibilities

- you are responsible for the content of the documents you place on Thrive and you have the ability to moderate any information as necessary
- You should report breaches of this AUP to the administrator, who may withdraw access to the secure area and/or report such incidents to the offender’s line manager

Passwords

Passwords are crucial to the security of the information and are a first line barrier against unauthorised access, so the longer and more complex they are and the more frequently changed, the better. Given the sensitivity and confidentiality of the information that is to be placed on Thrive, strong/complex passwords are used.

- A password should be a minimum of 6 Characters in Length
- A Password MUST contain at least 3 out of the 4 different Character Type requirements
    - An Upper case letter
    - A lower case letter
    - A number
    - A special character such as ~ ! @ # $ % ^ & * _ - + = ` | \ ( ) [ ] { } : ; ” ’ < > , . ?/
- Passwords cannot contain the username or parts of the username that exceed two consecutive characters e.g. if your account name or full name is ‘jamas’ then your password can contain ‘ja’ but not ‘jam’
- Each time a user updates their password it should be unique to ensure your account is kept secure e.g. no sequential passwords after a change so you cannot use ‘Password01’ then ‘Password02’
- Passwords should be changed every 30 days to ensure they remain secure

I have read, understood and will comply with this Acceptable Use Policy	**Name (print name):**
Signed:	
Date:	