Document Title	Learner Acceptable Use Policy (AUP)
Type of document	Corporate
Brief summary of contents	To provide: • Clear guidance for learners in the use of IT equipment • Additional information on Acts of Parliament • Responsibilities of learners when using Group systems
SLT member responsible for policy	Tony De'Ath
Date written	8th August 2016
Date last revised	4th November 2019
This document replaces	NNC Student computer use and Internet access policy, RC student AUP, DVC student AUP
Approval route/consultation	Department Head, SLT member
Head of Department (HOD) responsible for policy	Chris Muffett
Author of policy	Ian Headley
Contact details	ianheadley@rnngroup.ac.uk
Publication location	Public and portals
Date of final approval	24th August 2016
Date policy becomes live	31st July 2016
Review period	Annual

Links to external standards	ICO, relevant Acts of Parliament as detailed, Government guidance as detailed
Related documents	• Core (British) values guide for learners • Prevent strategy • KCSIE • RNN Group Data Protection Policy • Disciplinary policy and procedures (learners) • RNN Group Safeguarding Policy • BYOD policy • Student behaviour disciplinary procedure • Unsupervised students in classrooms policy • RNN Group CCTV policy • Privacy policy
Keywords	IT, ICT, Technology, Acceptable Use, Mobile Phones, Texting, BYOD, Email, Internet, Telephones, Data Protection, Legislation, Password, Safeguarding, Monitoring
Training needs	eSafety

This document is only valid on the day of printing

Controlled Document
This document has been created following the RNN Group policy production guidelines. It should not be altered in any way without the express permission of the author or HOD detailed above.

Learner Acceptable Use Policy (AUP)

Version 1.5

4th November 2019

Version Control Table

Date	Version No	Summary of Changes	Changes Made By
8th August 2016	1.0	Birth of policy	Ian Headley
22nd August 2016	1.1	Political statement amended, Section 8 General Points	Ian Headley
12th July 2017	1.2	SLT lead change Inclusion of password standards (Section 12) Creation of Section 17, Good Password Structure Additional guidance on Prevent & British Values (Section 16) Legislation update	Ian Headley
8th May 2018	1.3	Changes made to Data Protection Section 14 to reflect new legislation Other minor changes throughout the document in relation to the lawful basis for processing of personal information	Ian Headley
15th March 2019	1.4	Annual review, minor wording changes such as College replaced by Group Additional detail regarding safeguarding monitoring	Ian Headley
4th November 2019	1.5	Annual review	Kelly Condon

All or part of this document can be released under the Freedom of Information Act 2000

Table of Contents

Appendices

1 The aim of this policy

1.1 to encourage Learners to make good use of the educational opportunities presented by the Group's IT facilities and Internet access along with other electronic communications.

1.2 to safeguard and promote the welfare of Learners by preventing "cyberbullying" and other forms of abuse.

1.3 to provide good practice guidelines to Learners when using computer systems.

1.4 to minimise the risk of harm to the assets and reputation of the Group.

1.5 to provide Learners with the information and guidance they need to remain safe when working on computers/systems and the Internet.

1.6 to help Learners take responsibility for their own e-safety.

1.7 to ensure that Learners use technology safely and securely.

1.8 to provide information on various Acts of Parliament affecting the Learners use of IT systems and the Internet.

2 **Summary of this policy**

Learners must NOT

2.1 use the Internet connection for illegal, inappropriate, or obscene purposes, or in support of such activities. Illegal activities shall be defined as a violation of the law. Inappropriate use shall be defined as a violation of the intended use of the Group’s networks, and/or purpose and goal. Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly owned and operated communication vehicle.

2.2 create or transmit (other than for properly supervised and lawful research purposes) any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

2.3 use the network for any illegal copyright activity, including violation of copyrights or other contracts violating such matters as institutional or third party copyright, licence agreements and other contracts.

2.4 intentionally disrupt network server traffic or crash the network and connected systems.

2.5 create or transmit material that is designed or likely to cause annoyance, inconvenience or needless anxiety.

2.6 degrade or disrupt equipment or system performance on the Group’s networks.

2.7 use computing resources for commercial or financial gain or fraud (unless this is as part of a classroom led activity).

2.8 transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where that material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.

2.9 create or transmit defamatory material.

2.10 steal data, intellectual property or equipment.

2.11 gain or seek to gain unauthorised access to resources, files or entities.

2.12 use an account owned by another user.

2.13 wastefully use finite resources.

2.14 post anonymous messages.

2.15 download, install, run security programs or utilities that are designed to reveal weaknesses in the security of Group’s systems, or any other system.

2.16 misuse networked resources in any other way, such as the introduction of viruses.

2.17 attempt to bypass any network restrictions that are there to protect users.

3 Technology relating to this policy (but not restricted to)

3.1 'Computing' based technologies (such as PC's, laptops, tablets or mobile devices of any nature), whether physical or remotely accessed.

3.2 e-mail.

3.3 the Internet.

3.4 Virtual Learning Environments (VLE).

3.5 social networking or interactive web sites/software/content management systems for example Twitter, Facebook, Instagram, Tumblr, WordPress.

3.6 gaming sites, instant messaging, chat rooms, blogs and message boards.

3.7 mobile phones with the capability for recording and/or storing still or moving images.

3.8 webcams, video hosting sites (such as YouTube).

3.9 personal music players (such as iPods).

3.10 handheld game consoles.

3.11 interactive whiteboards.

3.12 other photographic or electronic equipment.

It applies to the use of any of the above on Group premises (or Group delivery location) and any use, whether on or off Group premises, which affects the welfare of other learners or where the culture or reputation of the Group are put at risk.

4 Authorisation

Internet access is provided to all Learners as a freely available service that does not require authorisation. To equip Learners with the knowledge they need to keep themselves safe on the Internet, all Learners are required to complete the eSafety module on the VLE for their own benefit and understanding of safely working online.

5 Compliance and Sanctions

It is every Learner's responsibility to ensure they comply with this policy. Abuse of access to systems may lead to the withdrawal of all network access and/or other Group systems.

Where violation of these conditions is illegal and/or unlawful, or result in loss or damage to the Group, the matter will be referred for the appropriate disciplinary or legal action.

6 **Definitions**

Cyber bullying: Cyber bullying is the misuse of digital technologies or communications to bully a person or a group, typically through messages or actions that are threatening and/or intended to cause offence, anxiety or humiliation. (see Kidscape: "Advice, what is Cyber bullying" as recommended by the Department for Education).

Examples of cyber bullying can include but are not limited to:

- Abusive comments, rumours, gossip and threats made using digital communications and/or technologies – this includes internet trolling.
- Sharing pictures, videos or personal information without the consent of the owner and with the intent to cause harm or humiliation.
- Hacking into someone's email, phone or online profiles to extract and share personal information, or to send hurtful content while posing as that person.
- Creating dedicated web sites that intend to harm, make fun of someone or spread malicious rumours.
- Blackmailing or pressurising someone to do something they do not want to.

E-safety means limiting the risks that Learners and young people are exposed to when using technology, so that all technologies are used safely and securely.

Protocols: Learners should comply with rules and protocols set by the Group, regarding, but not limited to, the following areas:

- E-mail and Internet.
- Mobile phone.
- Camera, photograph and video.
- Other electronic equipment.
- Communication between staff and Learners.

Sanctions may include:

- Increased monitoring.
- Confiscation: unacceptable use of electronic equipment could lead to confiscation of same.

Procedures: Learners are responsible for their actions, conduct and behaviour on the Internet in the same way that they are responsible during taught sessions, periods of self-study or at break times. Use of any technology should be safe, responsible and lawful. Any misuse of the Internet will be dealt with under the Group's Behaviour Policy. If you witness misuse by other Learners talk to a member of staff as soon as possible.

Learners must not use their own or the Group’s technology to bully others. Bullying incidents involving the use of any technology will be dealt with under the Group’s Anti-Bullying Procedures. If you think that you might have been bullied or if you think another person is being bullied, speak with a member of staff as soon as possible.

If there is a suggestion that a Learner is at risk of abuse, the matter will be dealt with under the Group’s Child Protection Procedures. If you are worried about something that you have seen on the Internet, speak with a member of staff about it as soon as possible.

The liability of the RNN Group: Unless negligent under the terms of this policy, the Group accepts no responsibility to the Learner or parents/guardians caused by, or arising out of, a Learners use of mobile phones, e-mail and the Internet whilst at a Group delivery location.

7 Social Media

Millions of people use social media on a daily basis across the world. The following guidance seeks to help Learners avoid the potential pitfalls of sharing information on the various social media sites, blogging sites and other similar networks.

The best advice that can be given is to employ common sense at all times to help keep yourself safe and to protect your own reputation and that of the Group itself.

Think before you post!

The RNN Group does not impose a blanket ban on the use of social media on its premises but expects that Learners in the library, computer rooms and common areas respect that the computers are provided primarily to support and facilitate your study and learning. For this reason, social media should not be used when a computer is needed by another Learner for academic purposes and the use of social media should be restricted to breaks in study or learning, unless this access constitutes to a part of the learning process as defined by the relevant teaching staff.

The RNN Group cannot control the access and use of social media on personal devices when utilising data provided over a mobile network nor can it control use by Learners off-site and out of Group operating hours. However, should any material come to the Group's attention that is defamatory, derogatory, offensive, abusive, bullying or in any way contravenes the ethos or reputation of the Group, we shall act in accordance with the relevant policy on behaviour, anti-bullying, discipline, suspension and exclusion.

Social media do's and don'ts

Do not use social media for non-academic purposes on the Group's computers during the day other than during lunchtimes and when there is no requirement from another Learner of the Group to use the computer for academic purposes. Learners should also avoid using social media on their own devices unless this is part of their learning, except at lunch time and social media should NEVER be used during taught session time, unless this is as part of a classroom led activity.

- Do not ask teaching staff or other Group staff members to be social media contacts such as Facebook friends, using their personal accounts. You will be placing them in a difficult position professionally.

- Before you post something, do think – would you say that out loud to or about the person, thing or organisation you are commenting on. If not, do not post it.

- Do keep details of your relationships to yourself.

- Do not be cryptic. Others may not be able to read between the lines you intend. If you have something to say, say it, but think before you post.

- Do talk to your parents or guardians before you open an account on Facebook. Facebook sets a minimum age of thirteen but your parents may still want to discuss with you how you are going to use it safely.

- Do consider how you present yourself on social media. Always express your own views and do not refer to other people's personal views in your posts.

- Do consider whether the contents of your post would be more appropriate in a private message.

- Do not share personal information on posts for example, names, email addresses, home or work addresses and phone numbers.

- Do familiarise yourself with the relevant social media sites privacy settings so that you can restrict access to information you consider personal. If you are not sure how to restrict access to certain groups of people, you should act as though all your information is available to everyone or get advice on privacy settings from someone you trust.

- Do not post anything that may offend, insult or humiliate others, particularly based on their sex, age, race, colour, national origin, religion, sexual orientation, disability or learning needs.

- Do not post anything that could be seen as threatening, intimidating or abusive. Offensive posts or messages can be seen as cyber-bullying. The Group’s anti- bullying and behaviour and discipline policies will apply to Learners found to be cyber-bullying.

- Do not impersonate any other person or use anyone else's social media account. This may be done as a joke but could upset the account holder or others. It is also an invasion of privacy.

- Do ask friends first before tagging them in photos. They may not want to be tagged or may be unhappy to be shown taking part in a particular activity. Write to your friends to let them know you have uploaded photos and they can decide whether to tag themselves or not.

- Do not use swear words on social media as this reflects badly on you and the Group.

- Do consider the appropriateness of your profile picture. Facebook, for example, will display your profile picture even when your information is set to private. If you do not want your profile picture to be viewed, do not upload one.

- Do consider whether you know someone well enough before you add them as a friend. Do not add someone if you do not want them to view your profile.

- Review and edit other people's comments, posts and tagged photos on your social media accounts. While you may be diligent in ensuring your account is appropriate, it is possible that you may receive inappropriate comments, pictures or videos from your friends.

- Be aware that material published online can remain online for a long time. In fact, they can be around forever. Remember that future friends, colleagues, employers, Universities etc. will be able to find your posts on line for several years to come. Forever is a long time. This is particularly true if you are posting about someone else.

- Do not use social media to criticise or complain about the Group. We welcome comments and complaints but these should be made through the appropriate channels.

Please THINK BEFORE YOU POST AND DON’T OVER-SHARE!

8 General Points

The RNN Group has the right to monitor any and all aspects of its computer systems that are made available to you and to monitor, intercept and/or record any communications made by Learners, including email or Internet communications in line with current legislation.

Details of sites visited, filtered and/or blocked under the Prevent Duty or Investigatory Powers Act 2016 may be released to authorised staff for investigatory purposes and may, in certain circumstances, be used in disciplinary action or provided to the relevant authorities. See section 15.

Learners are not required to provide consent to the monitoring of activities performed by RNN Group authorised staff, this data is processed within the legitimate business interests of the Group and for your and others vital interests or in the public interest.

The RNN Group has appropriate monitoring and filtering systems in place to support our safeguarding responsibilities as detailed in the Keeping Children Safe in Education (KCSIE) and Prevent Duty guidance. This level of monitoring is proportionate for safeguarding purposes at the Group's sites, even if the Internet services are being provided by a third party.

The Group constantly monitors its networks, when a 'safeguarding' keyword is detected, whether in an application, typed in an email, on social media, in a search engine, present on a web site or in a URL, the incident is captured. This capture is timestamped and logged with a screenshot, or video clip, to provide 'who, what, where' style information, putting the incident into context.

These captures are forwarded to the authorised teams within the Group for any appropriate action to take place. These alerts may be sent by email, active pop-ups or via regularly scheduled summary reports, so that issues can be addressed.

Within the alert, appropriate Group staff will see detailed records of IT usage, including captures, to facilitate an informed decision regarding the next steps to take. Informed with the relevant information, staff may then open up dialogues with the user and provide the appropriate safeguarding response.

This monitoring approach is centred on identifying people at risk and tackling any issues head on before they escalate. When the appropriate response has been actioned, staff may record it on the Group's systems for future reference. This complete log of information enables the Group to see patterns of concerning behaviour and address them with the appropriate support, based on the relevant issues.

If you require further information in this regard, the UK Safer Internet Centre has produced guidance for schools and colleges in England on "Appropriate Monitoring" - in response to the new statutory DfE guidance in "Keeping Children Safe in Education".

Computers, data stored on them (or the network) and RNN Group email accounts are the property of the Group and are designed to assist in the learning process. Learners should, therefore, have no expectation of privacy in any data stored or email sent or received on these systems, whether it is of an educational or personal nature.

E-mail and web site addresses within the RNN Group (including College sites) may change from time to time. Closed Circuit Television (CCTV) is in operation on Group premises for site safety and the security of employees, Learners and the general public.

Whilst using RNN Group provided computer systems, Learners must only engage in political discussions when this is part of their course, programme of learning or part of a classroom led activity where Learners discuss and debate issues in a considered way, showing respect for others ideas and points of view and does not favour any particular political party or faith.

9 Use of email

Emails should be drafted with care. Due to the informal nature of email, it is easy to forget that it is a permanent form of written communication and that material of this nature can be recovered, even when it is deleted from computers.

Learners should not make derogatory remarks in emails, any written derogatory remark may constitute libel. Learners requiring clarification in this regard should contact their tutor.

Learners must not create email congestion by sending trivial messages or unnecessarily copying of emails, this includes the initiation and propagation of chain emails. Learners should regularly delete unnecessary emails to prevent over-burdening the system.

If you do choose to use the RNN Group’s email systems for personal use, care should always be taken regarding the size of the email being sent and sizes should always be kept to the minimum possible. The content of personal emails must comply with the restrictions set out in these guidelines and in line with current legislation.

By sending emails on the Group’s systems, personal information may be being processed. If Learners do not wish the RNN Group to process such data, alternative communication means should be used.

Learners should be aware that all emails can be recovered, even after deletion and could be used as evidence in disciplinary or legal proceedings.

10 Bring Your Own Device (BYOD)

In using your own device on RNN Group networks, you are accepting the BYOD Acceptable Use Policy (AUP), acceptance of same will be required before use.

When you use your own device, the RNN Group does not guarantee that you will be able to use every online or networked facility it provides to its own equipment. The RNN Group accepts no responsibility for personal devices.

The RNN Group reserves the right to prevent access to any of its systems.

Personal data is transmitted at the risk of the person sending same.

Personal devices accessing the RNN Group’s network should have the appropriate security and protection measures in place, this will include, but not restricted to, the relative security updates applied and security software installed to protect other users, for example anti-virus software.

The RNN Group in no way takes responsibility for any fault or error incurred on personal devices by the use of its systems, rectification and/or repair will remain the responsibility of the device owner.

It is the individual’s responsibility to ensure that all use of personal devices complies with the RNN Group’s policies on Prevent, eSafety, copyright, Data Protection and handling of sensitive information.

11 Copyright and Downloading

Copyright applies to all text, pictures, video and sound, including those sent by email or available on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

Copyrighted software must never be downloaded. Such copyrighted software will include screen savers.

The RNN Group does not specify a maximum file size that Learners are permitted to download, but it does expect common sense to prevail when downloading files. This includes the downloading of large format images and multimedia files or streaming content such as games or films.

RNN Group Learners should not import non-text files or unknown messages on to the Group's systems without having them scanned for viruses. If Learners are in any doubt as to the sender or content of a file or message, then files should not be imported.

12 General Computer Usage

Learners are responsible for safeguarding their passwords for the Group's systems. For reasons of security, individual passwords should not be printed, stored on-line or given to others. User password rights given to Learners should not give rise to an expectation of privacy.

Passwords are an important aspect of computer security and are the primary authentication method for access to IT resources. The Group's standards for password creation is set to a minimum of sixteen characters, with no expiry. See section 17 for advice and guidance for good practice in password creation.

Learners who have partial access to a system must not attempt to gain access to functions for which they have no authority.

A Learners ability to connect to other computer systems throughout the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. Learners should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

Learners who observe practices contrary to any parts of this policy must report them to their tutor or another member of RNN Group staff at the earliest opportunity.

All Learners will be required to agree to this AUP at logon.

13 Software Installations / Copying

It is a criminal offence, and contrary to the RNN Group's policy, to install software for which the Group is not in possession of a bona fide licence.

Taking copies of copyrighted software is illegal and is prohibited by the RNN Group.

14 Data Protection

14.1 RNN Group data privacy notice

What we need

The RNN Group is what is known as 'the controller' of the personal data you provide to us. We collect not only basic personal data about you, things like your name, address, email etc. but may sometimes need to collect some special categories of information such as ethnic origin, data concerning health etc.
The RNN Group has a Data Protection Officer, the DPO can be contacted directly by emailing IG@rnngroup.ac.uk.

Why we need it

We need to know your basic personal data in order for us to provide you with details regarding your interaction with the RNN Group. We may also have legal obligations under UK legislation to collect data from you and will always process data where your vital interests are concerned or if it is in the public interest to do so. We will not collect any personal data from you that we do not need in order to provide and oversee any services to yourself.

What we do with it

All of the personal data we collect is processed by our staff in the UK however for the purposes of IT hosting and maintenance, this information may be located on servers within the European Union and occasionally, trusted parties outside the EU may have access to certain parts of the data we collect. No third parties have access to your personal data unless UK legislation allows them to do so or an official processing agreement is in place with the RNN Group. A full copy of our privacy policy is available on our web site www.rnngroup.ac.uk.

How long we keep it

There are various retention periods set for the Group, some relating to UK legislation, the data we collected will be destroyed or anonymised when these dates are reached. Your information that we use for marketing purposes will be kept until you notify us that you no longer wish to receive this type of information. More information on our data retention schedule can be found online at www.rnngroup.ac.uk.

What we would also like to do with it

The RNN Group may use some of the data that we have collected, such as your name and email address, to inform you of our future offers and similar products. This information is not shared with, or sold to, third parties and you can unsubscribe at any time via the unsubscribe option, phone or on our web site. Sometimes this data will be stored outside of the EU.

What are your rights?

We will not always need consent to use your personal information, for example, if we need it to meet regulatory requirements. Sometimes however, your express consent will be required, for example if we are collecting data regarding your health, this will be explained when we collect the data.

If at any point you believe the information we process on you is incorrect, you can request to see this information and even have it corrected or deleted, simply email dsar@rnngroup.ac.uk outlining your specific requirements.

If you wish to raise a complaint on how we have handled your personal data, you can contact our Data Protection Officer who will investigate the matter, contact details below.

If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law, you can complain to the Information Commissioner's Office (ICO). www.ico.org.uk.

15 Legislation

Legislation covered within this policy:

Investigatory Powers Act 2016 (previously known as The Regulation of Investigatory Powers Act 2000 (RIPA))

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Lawful Business Regulations)

The Data Protection Act 2018

Freedom of Information Act 2000

The Human Rights Act 1998

The Privacy and Electronic Communications (EC Directive) Regulations 2003

The Counter-Terrorism and Security Act 2015

The Computer Misuse Act 1990

The Terrorism Act 2006

Privacy and Electronic Communications (EC Directive) Regulations 2003 and amendment to the Regulations 2011

Police and Justice Act 2006

Crime and Disorder Act 1998

The Protection of Freedoms Act 2012

Serious Crime Act 2015

Copyright, Designs and Patents Act 1988

Equality Act 2010

Limitation Act 1980

Malicious Communications Act 1988

Digital Economy Act 2017

Prevent Strategy 2011

The Care Act 2014

The Children Act 1989 and 2004

Education Act 2002

Keeping children safe in education 2016 (Education Act 2002)

Childcare Act 2006

16 Linked policies and Guidance

RNN Group Data Protection Policy

RNN Group Data Subject Access Request (DSAR) Policy

BYOD AUP

RNN Group CCTV Policy

Privacy Policy

Cookies Policy

Disciplinary policy and procedure (learners)

Harassment policy

RNN Group Safeguarding policy

Student behaviour disciplinary procedure

Unsupervised students in classroom policy

Core (British) values guide for learners

Kidscape: "Advice, what is Cyber bullying"

What is the Counter Terrorism Act?

The Counter Terrorism and Security Act 2015 has introduced the Prevent Duty for various bodies including all FE colleges, adult education providers and independent learning providers with SFA funding or with over 250 students enrolled. Ofsted include Prevent compliance and engagement in all inspections.

What is the Prevent Duty?

Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on all FE and training providers, as listed in Schedule 3 of the Act, to have "due regard to the need to prevent people from being drawn into terrorism".

The Prevent duty is also part of the Safeguarding duty for providers but one that extends to all learners of all age groups and also staff.

What are British Values?

British values are defined as "democracy, the rule of law, individual liberty and mutual respect and tolerance for those with different faiths and beliefs"; institutions are expected to encourage students to respect other people with particular regard to the protected characteristics set out in the Equality Act 2010.

What is Extremism?

The government has defined extremism in the Prevent strategy as: "vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs." This also includes calls for the death of members of the British armed forces.

17 Good Password Structure

Password entropy is a measurement of how unpredictable a password actually is.

Password entropy is based on the characters used (uppercase, lowercase as well as symbols) including password length. It predicts how difficult a given password would be to crack through guessing, brute force cracking, dictionary attacks or other common methods.

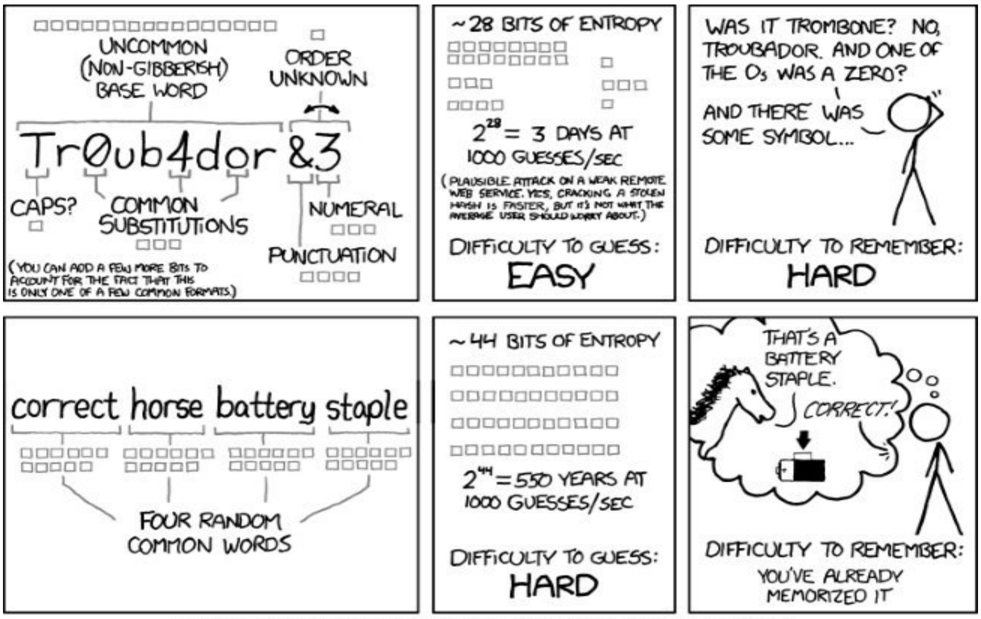
Password entropy is usually expressed in terms of bits, a password that is already known has zero bits of entropy, one that would be guessed at the first attempt half the time would have 1 bit of entropy. A passwords entropy can be calculated by finding the entropy per character multiplied by the number of characters in the password itself.

Of course, password entropy cannot be the only thing considered or passwords would be too long, too complex and unmemorable.

Best password practices involve employing something memorable to the user but not easily guessed by anyone else. Because password length is one of the most important factors affecting password entropy and overall strength, a longer password can be simpler than a shorter one and still be effective, as you can see from the demonstration graphic within this policy section.

Therefore, using all of the structures available to us, we can create an extremely strong password that can easily be remembered for example:

Correct horse battery staple 2017


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.