Staff (and Volunteer) Acceptable Use Policy Agreement
United Schools Federation Policy
This Acceptable Use Policy is intended to ensure:
- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that ICT systems and users within the United Schools Federation are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that staff are protected from potential risk in their use of ICT in their everyday work.

Acceptable Use Policy Agreement
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:
- I understand that the United Schools Federation will monitor my use of the ICT systems, email and other digital communications, and that the federation has the right to access such systems for disciplinary investigations and for collating data as part of a subject access request (e.g. request for personal data), or a Freedom of Information or Environmental Information Regulation request (e.g. request for school data)
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the parameters agreed by the United Schools Federation.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password (other than the ICT Co-ordinator/Technician).
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to either the ICT technician/ICT Co-ordinator or the Principal.

I will be professional in my communications and actions when using school ICT systems:
- I will use reasonable controls to safeguard the use of personal devices (personal devices are devices which are not managed and owned by the school). Such controls are:
- Personal devices are protected by a PIN/Password/Fingerprint and encrypted where possible,
- Do not leave webmail logged in on a personal device
- Attachments on personal devices are not opened unless in an emergency (as these download to the telephone).
- I will not process or store any school personal data on the personal device, I will instead work on, process and store the data on the school network (e.g. OneDrive, SharePoint)
- I will lock screens when my device is unattended (which can be done by pressing + L)
- I will reference the new Data Protection Act 2018 and GDPR where necessary.
- I will only open attachments or click on links on emails that I am expecting and if they do not look or feel right I will check with the sender by other trusted means (e.g. telephone call or SMS).

- I will ensure special categories of personal data *(data relating to race/ethnicity, religion, genetics, health, photos, sexual orientation, trade union, political opinions)* is given extra security, and at a minimum is locked away when not in use and is kept on my person when transporting it offsite (when it is in unencrypted form e.g. paper)
  - I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
  - I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
  - I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
  - I will not use chat and social networking sites in school in accordance with the United Schools Federation's policies.
  - I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
  - I will not engage in any on-line activity that may compromise my professional responsibilities.

The United Schools Federation and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
  - When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the United Schools Federation about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
  - I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.
  - I will ensure I blind copy (BCC) when emailing multiple external recipients (e.g. parents)

  - I will ensure that my data is regularly backed up, in accordance with relevant school policies.
  - I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
  - I will take measures to ensure personal data is protected when emailing an external recipient. Either by the use of a pseudonymisation, anonymisation, encrypting the information within an attachment – and communicating the password by other trusted means (e.g. SMS, phone call, or pre-agreeing it), or using a secure email product (for example - Egress)
  - I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
  - I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, without consultation with the ICT Co-ordinator or technician.
  - I will not disable or cause any damage to school equipment, or the equipment belonging to others.

Name …………………………………………………… Signed …………………………………………………………………………………….

Date …………………………………………………………………….

Reviewed 8th October 2020   Next review October 2022