



## **E-Safety - Staff and Volunteer Acceptable Use Policy**

### **School Policy**

This Acceptable Use Policy reflects the school e-safety policy. The school will ensure that staff and volunteers will have good access to ICT to enable efficient and effective working, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users. This policy is to be read in conjunction with the GDPR policy.

### **Scope of Policy**

This Acceptable User Policy (AUP) policy applies to staff, volunteers and guests who have access to and are users of school ICT systems and to school related use of ICT systems outside of school.

### **My Responsibilities**

I agree to:

- read, understand, sign and act in accordance with the School e-safety policy
- report any suspected misuse or concerns to the e-safety Leader
- monitor ICT activity in lessons, extracurricular and extended school activities
- model the safe use of technology
- demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks making sure that these are in line with school ethos and policies especially at the time of a Critical Incident

### **Education**

I agree to:

- provide appropriate e-safety learning opportunities where appropriate as part of a progressive e-safety curriculum
- respect copyright and educate the pupils to respect it as well

### **Training**

I agree to:

- participate in e-safety training
- request training if I spot an opportunity to improve on my professional abilities

### **Cyberbullying**

I agree to:

- ensure the schools zero tolerance of bullying. In this context cyberbullying is seen as no different to other types of bullying.
- report any incidents of bullying in accordance with school procedures

### **Technical Infrastructure**

I understand that the school will monitor my use of computers and the internet. I will not try to by-pass any of the technical security measures that have been put in place by the school. These measures include:

- the proxy or firewall settings of the school network (unless I have permission)
- not having the rights to install software on a computer (unless I have permission)

### **Passwords**

- I will only use the password(s) given to me
- I will never log another user onto the system using my login

### **Filtering**



- I will not try to by-pass the filtering system used by the school
- If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised
- I will report any filtering issues immediately

### **Data Protection**

I understand my responsibilities towards the Data Protection Act and will ensure the safe keeping of personal data at all times.

I will always lock/logout my Computer/Device when left unattended

### **Use of digital images**

I will follow the school's policy on using digital images especially in making sure that only those pupils whose parental permission has been given are published.

### **Communication**

I will be professional in all my communications and actions when using school ICT systems.

### **Email**

I will use the school provided email for all business matters.

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 programmes).

### **Social Media and Personal Publishing**

I will ask permission before I use social media with pupils or for other school related work.

I will follow the e-safety policy concerning the personal use of social media.

On any personal accounts I will not post any comments about any pupil and not post disparaging remarks about my employer/colleagues.

When there is a Critical Incident I will not post any comments online.

I will follow the agreed Policy/Procedure when posting to the School's Social Media accounts

### **Mobile Phones**

I will only use my personal mobile phone for use with educational applications during contact time with pupils.

I will not use my personal mobile phone to contact pupils or parents.

### **Reporting incidents**

I will report any incidents relating to e-safety to the e-safety Leader or ICT Technician.

I will make a note of any incidents in accordance with school procedures.

I understand that in some cases the Police may need to be informed.

### **Sanctions and Disciplinary procedures**

I understand that there are regulations in place when pupils use ICT and that there are sanctions if they do not follow the rules.

I understand that if I misuse the School ICT systems in any way then there are disciplinary procedures that will be followed by the school.

---

### **Exemptions to the policy**

In line with the responsibilities and duties of the job description, the Senior IT Systems Technician may on occasions be required to undertake actions that are not in line with the acceptable use policy. These actions should only be undertaken if directed to do so by the Headteacher or Senior Leadership Team and can be fully justified.

***Cranborne Middle School***  
*Computing Acceptable Use Policies*  
*March 2021*



I have read and understand the full School e-safety policy and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name

---

Signed

---

Date

---