



# **E-Safety Policy**

**Last Updated: September 2023**

**To Be Reviewed: September 2025**

## **Introduction**

The School E-Safety Policy document covers all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti- Bullying policies.

The School E-Safety Policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

### **Development, Monitoring and Review of this Policy**

- This e-safety policy has been developed by a working committee made up of: Headteacher, ICT teacher and the Director of Education.
- The policy will be reviewed annually.
- The ICT Head of Department is the lead person on E Safety.
- E safety will be monitored by the Headteacher and the lead person

## **Scope of the Policy**

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

## **Roles and Responsibilities**

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

### **Governors**

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

### **Headteacher and Senior Leaders:**

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

### **E-Safety Coordinator/Officer:**

- leads the e-safety committee and/or cross-school initiative on e-safety
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to Senior Leadership Team and Safeguarding officer

#### **Technical staff:**

The E-Safety coordinator is also the network manager and is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets the e-safety technical requirements outlined in the E-Safety Policy and guidance.
- that users may only access the school's networks through a properly enforced password protection.

#### **Teaching and Support Staff**

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher/or Head of ICT for investigation/action/sanction

#### **Designated person for child protection/Child Protection Officer**

Should be trained in e-safety issues and be aware of the potential for serious child Protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying
- Extremist materials ( refer to Prevent Duty and Safeguarding Policy)

#### **Students/pupils:**

- are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Need to develop awareness and resilience in keeping safe through various forms of technology ( media, web, social networking etc) both at school and home

#### **Parents/Carers**

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy
- accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy.

### **Community Users**

Community Users who access school ICT systems or Learning Platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

### **E-Safety Education and Training**

#### **Education – students / pupils**

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT/PHSE/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

#### **Education & Training – Staff**

It is essential that all staff receives e-safety training and understands their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

## Good practice guidelines


### Email



**DO**

Staff should only use their school email account to communicate with each other





Check the school e-safety policy regarding use of your school email or the internet for personal use e.g. shopping



**DO NOT**

Staff: don't use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

## Images, photos and videos



### DO

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.



Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.



### DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.


## Internet



**DO**

Understand how to search safely online and how to report inappropriate content .





Staff and students/pupils should be aware that monitoring software will log online activity.



**DO NOT**

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.


## Mobile phones



**DO**

*Staff: If you need to use a mobile phone while on school business (trips etc), please use a Common Sense approach*





Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first



**DO NOT**

Don't retain service student/pupil/parental contact details for your personal use.



## Social networking (e.g. Facebook/ Twitter)

Best practice

### DO

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends to not post tagged images of you on their open access profiles.

Safe practice



Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Poor practice

### DO NOT

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.

Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.
- Don't accept ex-students/pupils users as friends.
- Don't write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.

## Incident Management

<b>Incidents (students/pupils):</b>  <i>(School to complete the table, adding other items or deleting items as appropriate)</i>	Refer to class teacher	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police/Prevent/Social	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)									
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone/digital camera / other handheld device									
Unauthorised use of social networking/ instant messaging/personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									
Attempting to access or accessing the school network, using another student's/pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means									

to subvert the school's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornography									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

<b>Incidents (staff and community users):</b>  <i>(School to complete the table, adding other items or deleting items as appropriate)</i>	Refer to Head of Department / Head of Year/Subject	Refer to Headteacher	Refer to Police/Prevent/Social	Refer to technical support staff for action re filtering / security etc	Removal of network / internet access rights	Warning	Further sanction <i>(please state)</i>
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)							
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email							
Unauthorised downloading or uploading of files							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account							
Careless use of personal data eg holding or transferring data in an insecure manner							
Deliberate actions to breach data protection or network security rules							
Corrupting or destroying the data of other users or causing							

deliberate damage to hardware or software							
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature							
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils							
Actions which could compromise the staff member's professional standing							
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school							
Using proxy sites or other means to subvert the school's filtering system							
Accidentally accessing offensive or pornographic material and failing to report the incident							
Deliberately accessing or trying to access offensive or pornographic material							
Breaching copyright or licensing regulations							
Continued infringements of the above, following previous warnings or sanctions							

## Appendix 1 – Student/Pupil AUP

### Student/pupil Acceptable Use Policy Agreement Template

This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following:

- I WILL** and
- I WILL NOT** statements.

If there's anything you're not sure of, ask your teacher.

#### **I WILL:**

- treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission
- be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- not use my mobile phone in school
- immediately report any damage or faults involving equipment or software, however this may have happened
- Not access social websites and inappropriate websites

This form relates to the student/pupil Acceptable Use Policy.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police and exclusion.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, Learning Platform, website etc

(Parents/carers are requested to sign the permission form below to show your support of the school in this important aspect of the school's work).

Name of Student/Pupil		
Class		
Signed (Student/Pupil)		Date
Signed (Parent/Carer)		Date

## **Appendix 2 – Staff, Volunteer, Community User AUP**

### **Staff, Volunteer and Community User Acceptable Use Policy Agreement Template**

#### **School Policy**

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for students' learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

#### **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 students/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 school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email 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 policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files or on Staffshare, without 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. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will refrain from using chat and social networking sites in school.
- I will only communicate with students/pupils and parents/carers using official school systems & emails. 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.
- 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.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not 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 use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not (unless I have permission) 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 programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.



- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority, dismissal and in the event of illegal activities the involvement of the police

**I have read and understood the School's E-safety Policy**

I have read and understand the above 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) within these guidelines.

Name	
Position	
Signed	
Date	

