

## **Acceptable Use Policy 2025-2026**



### **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 school systems and users 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 technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

### **Definitions**

#### **Undesirable materials**

- Pornographic images or obscene text on internet websites
- Language that is abusive, profane, inflammatory, coercive, defamatory, blasphemous or otherwise offensive, on Web sites or e-mail messages
- Racist, exploitative or illegal materials or messages on websites or e-mail

#### **Undesirable contacts**

- E-mail messages from unknown or unverified parties, who seek to establish a child's identity and/or to communicate with them, such as for advertising or potentially criminal purposes.

#### **Unacceptable use**

- Deliberate searching for and accessing of undesirable materials
- Creating and transmitting e-mail messages that contain unacceptable language or content
- Creating and publishing on the Internet materials that contain unacceptable language or content.

#### **Adults**

- School teaching staff
- Teaching assistants
- Non-teaching school staff
- Students
- Visitors and guests of the staff
- Parents

### **Unintentional Exposure of children to undesirable materials**

It is the school's policy that every reasonable step should be taken to prevent exposure of children to undesirable materials on the internet. It is recognised that this can happen not only through deliberate searching for such materials, but also

unintentionally when a justifiable internet search yields unexpected results. To prevent such occurrences, the school has adopted the following position:

The use of an Internet Service Provider which offers protection by

- The filtering of sites by language content with prohibition of sites with unacceptable vocabulary
- The imposition of a 'banned list' of undesirable sites

In-school protection by

- Adult supervision of pupils' internet activity, with no use of a computer allowed unless a suitable adult present
- You Tube only used as a whole class/group teacher tool and to be watched first, by teacher, prior to the lesson.
- Smoothwall Software purchased, installed and monitored on a weekly basis – weekly summaries are emailed to DSL and Computing Lead.

In the event of children being unintentionally exposed to undesirable materials the following steps will be taken:

1. Pupils should switch off their **Monitor** and notify a teacher immediately.
2. The teacher will ensure no pupils can see the monitor and will write down the website, date and nature of the material. The website can then be logged off.
3. The teacher will inform the ICT coordinator who will ensure the website is filtered out.
4. The teacher will record the incident in a central log, by which the school may be able to reliably report the frequency and nature of any incidents.
5. Parents or Governors will be notified at the discretion of the Head according to the degree of seriousness of the incident.

### **Intentional Access of Undesirable Materials by Children**

Children must never intentionally seek offensive material on the Internet. Any transgression should be reported and recorded as above. Any incident will be treated as a disciplinary matter and the parents of the child or children will normally be informed.

If deliberate access to undesirable materials is found to be repeated, flagrant or habitual, the matter will be treated as a serious disciplinary issue. The child's parents will be informed and the Governing Body will be advised.

### **Deliberate Access to Undesirable Materials by Adults**

Deliberate access to undesirable materials by adults is unacceptable and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual the matter will be treated as a very serious disciplinary issue. The Governors will be advised and the LEA will be consulted.

### **Receipt and transmission of e-mails by Children**

It is recognised that e-mail messages received or transmitted by children can contain language or content that is unacceptable. It is also recognised that some people may try to use e-mail to identify and contact children for unacceptable reasons.

To avoid these problems, the school has adopted the following practice:

- Pupils do not have access to e-mail except in teacher-controlled situations
- Pupils only use Purple Mash email tool or school email addresses for older children.

- Pupils do not read e-mail messages unless an adult is present or the message has been previewed by a teacher
- Steps are taken to verify the identity of any school or child seeking to establish regular e-mail with this school
- Pupils never send an e-mail message without having the contents approved by their teacher
- To avoid children revealing their identification within e-mail messages the child's address is never revealed and only the child's forename is given.

If staff believe that children have been targeted with e-mail messages by parties with criminal intent the message will be retained, the incident recorded and the Governors and the child's parents informed. Advice will also be given regarding further steps.

### **Publishing of materials on the Internet**

It is recognised that staff and children may at some time produce and publish materials on an internet website associated with the school or the County.

No materials will be published on the Internet which contain any unacceptable images, language or content. Infringement of this rule will be taken as a serious disciplinary issue.

No materials will be published on the Internet which reveal the identity of any child.

Identifiable, facial or close-up photographs of children will not be published on the Internet without individual parental approval.

### **Use of the Internet by staff and adult users**

It is expected that staff will also adhere to a code of responsible use of the internet and computers belonging to the school. Staff are expected to read and keep to the policy on Acceptable Internet Use for staff and adult users.

### **Use of the School Internet by Visitors and Guests**

Members of school staff will take responsibility for the actions of any adult guests or visitors who they allow or encourage to use the school Internet facilities. The essential "dos and don'ts" of this policy should be explained to such visitors and guests prior to their use of the Internet.

Unacceptable use will lead to the immediate withdrawal of permission to use the school internet facility.

### **Copyright Issues**

It is recognised that all materials on the Internet are copyright, unless copyright is specifically waived. It is the school's policy that the copyright of Internet materials will be respected.

Where materials are published on Internet as part of the teacher's professional duties, copyright will remain with the County Council. Materials published on school web sites will contain due copyright acknowledgements for any third-party materials contained within them.

### **Review of this policy**

This policy will be revised at a SLT meeting with the Computing coordinator, the outcome of which will be reported to the school governing body and staff. When approved by the Governing body each member of staff will have a copy of this policy and it will be available on the school intranet and website.

This policy has been explained to the pupils of the school so that they understand that there are dangers associated with internet use, and they know what behaviour is expected of them. Within classes, pupils have collaboratively drawn up internet safety rules, which are displayed within the classroom and computer suite.

### **Safeguarding / Child Protection**

All staff and Governors have received appropriate safeguarding and child protection training (September 2025). All staff have read the following:

- Keeping Children Safe in Education 2025
- What to do if you're worried that a child is being abused
- Staff Code of Conduct
- Safeguarding and Child Protection Policy

Other related policies have been signposted such as Working Together to Safeguard Children, Anti-Bullying, Anti-Cyber Bullying Policy, Behaviour Policy, Critical Incidents, Health & Safety etc.

Staff working with children should maintain an attitude of '*it could happen here*' where safeguarding is concerned. If staff have any concerns about a child's welfare, they should act upon them immediately. They should follow the school's policy and procedures and speak with the Designated Safeguarding Lead (Miss Crawford) or one of the Deputy Safeguarding Leads (Mrs Kelly, Mrs Moorhouse or Mrs Lawrence). In the absence of these staff members, a member of the SLT should be contacted. All concerns should be acted upon and recorded on CPOMS.

Next review date: September 2026