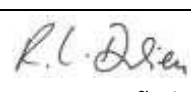




# E-Safety Policy

## 2026/27

|                                    |             |                            |                                                                                       |      |
|------------------------------------|-------------|----------------------------|---------------------------------------------------------------------------------------|------|
| <b>Policy Date:</b>                | August 2026 | <b>Version:</b>            |                                                                                       |      |
| <b>Policy Review Date</b>          | August 2027 | Mrs R Dulieu (Headteacher) |  | 11   |
| <b>Ratified by Governing Body:</b> |             |                            |                                                                                       |      |
| Name:                              |             | Signature                  |                                                                                       | Date |

## **Introduction and Overview**

### **Rationale**

#### **The purpose of this policy is to:**

- set out the key principles expected of all members of the school community at Barley Croft Primary School with respect to the use of Computing based technologies.
- safeguard and protect the children and staff of Barley Croft Primary School.
- assist school staff working with pupils to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice. □ set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

#### **The main areas of risk for our school community can be summarised as follows:**

##### **Content:**

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse; - Lifestyle websites promoting harmful behaviours, for example pro-anorexia/selfharm/suicide sites; Hate content;
- Content validation: how to check authenticity and accuracy of online content.

##### **Contact:**

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms; Social or commercial identity theft, including passwords

##### **Conduct:**

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information;
- Digital footprint and online reputation;
- Health and well-being (amount of time spent online (gambling, body image, internet or gaming);
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (selfgenerated indecent images);
- Copyright (little care or consideration for intellectual property and ownership – such as music and film). (Ref Ofsted 2013)

**Scope:**

This policy applies to all members of Barley Croft Primary School community (including staff, pupils, volunteers, parents /carers, visitors, community users) who have access to and are users of our school's Computing systems, both in and out of Barley Croft Primary School.

The Education and Inspections Act 2006 empowers Headteacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

**This policy should be read in line with the school's remote learning policy which sets out the school's procedures/protocols for remote learning.**

**1. Writing and reviewing the e-safety policy**

- The school appoints an e-safety Co-ordinator. This may be the Designated Safeguarding Lead / Computing Lead as the roles overlap
- Our e-safety policy has been written and agreed by staff and Governors.
- The e-safety policy will be reviewed annually.

**2. Teaching and Learning****2.1 Why internet use is important**

- The internet is an essential element in 21<sup>st</sup> century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

**2.2 Internet use to enhance learning**

- The school internet access is designed expressly for pupils to use and will include filtering appropriate to the age of the pupils.

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

### **2.3 Evaluating internet content**

- If staff or pupils discover unsuitable sites, the URL, time and date and content must be reported to the Computing Co-ordinators/technician
- The school will ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

## **3. Managing Internet Access**

### **3.1 Information system security**

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses the EMPSN broadband with its firewall and filters.

### **3.2 Published content and the school web site**

- The contact details on the web site are the school address and telephone number. Staff and pupils personal information will not be published.
- The Web site administrator (Kaelen McAtee ) will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **3.3 Publishing pupils images and work**

- Photographs which include images of pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' names will not be used anywhere on the web site, particularly in association with photographs.
- A form signed by parents or carers must be obtained before photographs of pupils are published on the school web site. (Written permission from parents)

### **3.4 Social networking and personal publishing**

- Social networking sites and newsgroups will be blocked. (unless a specific use is approved)
- Pupils are advised never to give out personal details of any kind which may identify them or their location.

### **3.5 Managing filtering**

- The school will work in partnership with Leicester City Council e-learning team to ensure that filtering systems are as effective as possible.
- If staff, students or pupils discover unsuitable sites, the URL, time and date must be reported to the school e-safety co-ordinator, the IT technician, then the LA.

### **3.6 Managing emerging technologies**

- ☐ Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

### **3.7 Protecting personal data**

- ☐ Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

## **4. Policy Decisions**

### **4.1 Authorising internet access**

- The school will maintain a current record of all staff and students who are granted internet access.
- All staff (and students) must read and sign the acceptable Computing use agreement and e-safety agreement form for school staff before using any school Computing resource.
- All Foundation Stage, Key Stage 1 & 2 access to the internet will be by adult demonstration with directly supervised access to specific approved on-line materials.

### **4.2 Assessing risks**

- In common with other media such as magazines, books and video, some material available on the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences of internet access.

- The headteacher will ensure that the e-safety policy is implemented.

#### **4.3 Handling e-safety complaints**

- Complaints of internet misuse will be dealt with by a senior member of staff/ Deputy Head or Headteacher.
- Any complaint about staff misuse must be dealt with in accordance with school child protection procedures.

### **5. Communication**

#### **5.1 Introducing the e-safety policy to pupils**

- Pupils will be informed that internet use will be monitored

#### **5.2 Staff and the e-safety policy**

- All staff will be given a copy of the school e-safety policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

#### **5.3 Enlisting parents' support**

- Parents will be informed about the school e-safety policy on the school web site, and in newsletters.
- The school will arrange presentations / information for parents regarding e-safety awareness as appropriate