

# William MacGregor Primary School



## Online Safety Policy

Ratified by staff and Governors - September 2017

Review date - September 2018

**Online Safety Coordinator:** Mrs Natalie Jones

**Designated Safeguarding Lead:** Mrs Suzie Sedgley - Head Teacher

**Deputy Designated Safeguarding Leads:** Ms Pauline Constantine/  
Mrs Natalie Jones

**Chair of Governors:** Mrs Woodhouse

**Governor for Online Safety:** Andy Hadley

### UNCRC

**Article 3:** The best interests of the child must be a top priority in all actions concerning children.

**Article 6:** All children and young people have the right to life. Governments should ensure that children and young people survive and develop healthily.

**Article 12:** Children and young people have the right to say what they think should happen, when adults are making decisions that affect them and to have their opinions taken into account.

**Article 33:** The Government should provide ways of protecting children and young people from dangerous drugs.

**Article 34:** The Government should protect children and young people from sexual abuse.

**Article 36:** Children and young people should be protected from any activities that could harm their development.

## **The purpose of the Online Safety policy.**

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to Online Safety. The policy relates to other policies including ICT curriculum, Internet Access, Bullying, Child Protection and Health and Safety.

## **Writing and reviewing the Online Safety policy**

The Online Safety Policy and its implementation will be reviewed annually by the Online Safety Coordinator, in collaboration with the Online Safety group and governor.

## **Teaching and learning**

### **Why Internet use is important**

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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.

### **Internet use will enhance learning**

- The school Internet access will be designed expressly for pupil use and will include filtering.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

### **Pupils will be taught how to evaluate Internet content**

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

## **Managing Internet Access**

### **Information system security**

- School ICT systems capacity and security will be reviewed regularly by Entrust<sup>1</sup>.
- Virus protection will be updated regularly by Entrust

### **E-mail content and the school web site**

---

<sup>1</sup> Entrust are continually monitored by Senior Leadership to ensure they are providing a good, value for money, service.

- Pupils may not use email in the school.
- The contact details on the Web site should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing pupil's images and work**

- Photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils work can be published on the school website or social media pages unless permission to do so has been refused by the pupil, their guardian or parents.

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

The school will deny access to social networking sites and students will be advised not to use these at home.

Staff should not accept or initiate friend/follow requests from pupils past or present (up until the age of 18) on social media sites. Staff should not accept or initiate friend/follow requests from parents of current pupils. New members of staff should remove children and parents from their social media pages upon taking their new role in accordance with the Acceptable Use Policy (please see the Acceptable Use Policy for Staff and Safeguarding Policy).

### **Managing filtering**

- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety coordinator at the earliest point. The 'Click CEOP' button can be pressed when working offsite to report any unsuitable sites. Staff can view the Online Safety flowchart for further guidance.
- Internet use is monitored each week through future digital (Entrust). Weekly emails (received by both the headteacher and the Online Safety coordinator showing internet activity is monitored and actioned by the Online Safety Coordinator. Online Safety governor to monitor actions and sign oversight sheet.

### **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.
- Mobile phones will not be used during school time.
- Staff will be very vigilant during sessions with Ipads as they are not monitored by Central Policy, however websites are still subject to the same server filtering.

## **Assessing risks**

The school will take all reasonable precautions to prevent access to inappropriate 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.

## **Handling Online Safety complaints**

- The Headteacher will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school Child Protection Procedures.
- The School regards Online Safety as a wider community issue and will deal rigorously with out of school Online Safety incidents that relate to members of the school community.

## **Community use of the Internet**

All use of the school internet connection by community and other organizations shall be in accordance with the Online Safety policy. Any community users will be required to sign and agree to the Acceptable Use Policy.

## **Introducing the Online Safety policy to pupils**

- Online Safety rules will be discussed with the pupils at the start of each year.
- Online Safety posters will be posted in a prominent place near all ICT equipment, so that all users can see them.
- Every class will have an Online Safety display.
- Each child will have a personal computer account and will use this when they access any school desktop computer or laptop.
- Pupils are informed that network and Internet use is monitored and appropriately followed up.
- The children will receive regular Online Safety lessons and are constantly reminded of online safety.
- Children will sign an acceptable use policy, yearly, before accessing any school device connected to the internet.

## **Staff and the Online Safety policy**

- All staff will have access to the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic will be monitored.
- Discretion and professional conduct is essential.
- Staff will always use the child friendly safe search engine, Kidrex, when accessing the web with pupils.
- Children should only use YouTube under supervision from a member of staff.
- All staff will sign an acceptable use policy.

## Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, and conversations.  
If using the internet at home:
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Students should only invite known friends and deny access to others.
- Parents will sign the acceptable use policy and their children will not be able to access any school device connected to the internet until this is done.

## William MacGregor Facebook page

Online social media tools can also be excellent tools for teaching and learning and can provide exciting, new opportunities for schools to engage, communicate and collaborate with pupils and the wider community. Our Facebook page has been 'live' since August 2013 and has been instrumental in celebrating and sharing our children's achievements. Our community has used our page to comment on the achievements of the children and school.

**Security** - School provided devices and tools are always used (e.g. work provided digital cameras, mobile devices, laptops etc.). Security settings are set so every post and comments are sent directly to the Head Teacher's email account so any inappropriate comments can be removed immediately and the person making the comment blocked. The Head Teacher has not had reason to remove a post or block a person yet. Permission is granted from parents before a child's image is uploaded onto our page. Only a child's first name is used.

## PREVENT

### Anti-radicalization and extremism

Radicalization refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

Extremism is defined by HM Government as 'Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths or beliefs: and/or calls for death of members of our armed forces, whether in this country or overseas'.

Through Future Digital we weekly monitor pupil and staff use of computers. Any suggestion or suspicions of any of the above would be actioned following the schools safeguarding procedures and Online Safety flow chart. Please also refer to the schools Prevent Policy.

