Greenleys Junior School

LEARNING for LIFE

# E-Safety Policy

| | |
|---|---|
| Date of Approval: | 8 November 2018 |
| Date of Next Review: | November 2019 |
| | |
| Signed: Executive Headteacher | M Talbot |
| Signed: Chair of Governors | M Hall |

**Introduction**

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety. It also aims to protect the reputation of employees of the school and the school as a whole from intended or unintended abuse via personal employee usage of social networking and personal internet sites. The school recognises that such sites are increasingly useful communication tools and acknowledges the right of employees to freedom of expression. However, employees must be aware of the potential legal implications of material which could be considered abusive or defamatory.

This policy should be read in conjunction with the Staff Code of Conduct.

**Writing and reviewing the e-Safety policy**

The school has a designated e-safety leader.

The e-Safety policy has been agreed by the senior management team and approved by the governors. It will be reviewed on an annual basis.

**Teaching and Learning**

- The purpose of internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Access to the internet is a necessary tool for staff and students.
- It helps to prepare students for their on-going career and personal development needs.
- It is a requirement of the National Curriculum (NC) orders for computing and is implied in other subject areas.
- The school has its own E-Safety rules which the children follow.

**Internet use to enhance learning**

- Internet access is provided by Armstrong Bell. This includes filtering appropriate to the content and age of pupils.
- Internet access is planned to enrich and extend learning activities.
- Access levels are reviewed to reflect the curriculum requirement.
- Pupils are given clear objectives for internet use and sign an Internet Agreement.
- Staff select sites which support the learning outcomes planned for pupils' age and maturity.
- Pupils are taught how to take responsibility for their own internet access.

**Pupils are taught how to evaluate internet content**

- Pupils are taught ways to validate information before accepting that it is necessarily accurate.
- Pupils are taught to acknowledge the source of information, when using internet material for their own use.
- Pupils are made aware that the writer of an e-mail or the author of a Web page might not be the person claimed.
- Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
-

## Managing internet access

### Information System Security

- Virus protection is updated automatically.

### E-mail

- Pupils are encouraged to use their school email account.
- Pupils must tell a teacher immediately if they receive offensive email.
- In emails, pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission.
- Pupils are taught not to open suspicious incoming email or attachments.
- The forwarding of chain letters is not permitted.

### Published content and the school web site

- The website complies with the school's guidelines for publications.
- All material must be the author's own work or where permission to reproduce has been obtained, it is clearly marked with the copyright owner's name.

### Publishing pupils' images and work

- Photographs must not identify individual pupils.  Group shots or pictures taken “over the shoulder” are used in preference to individual “passport” style images.
- Children's photographs are only allowed to go on the website once permission has been received from the child's parents.
- Children’s work which contains photographs must not also contain the child’s name.

### Social networking and personal publishing

- Pupils will not be allowed to access public chat rooms without supervision.
- Pupils will be taught the dangers of using these ‘chat rooms’.

### Managing filtering

- SLT ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing Subject Leader who will then investigate further and block access to these sites if needed.

### Managing technologies

- Mobile phones must not be used by children in school.
- The sending of abusive or inappropriate text messages is forbidden.
- School cameras are used by both staff and children for educational purposes.

### Protecting personal data

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

### Definition of Online Presence

This policy applies to personal use of social networking sites (for example: Facebook, Twitter, Instagram etc.), personal web pages, personal space provided by internet providers and internet presence including blogs which make available personal views to the general public, including web pages or social media pages hosted by Milton Keynes Council which you are visiting as a personal user (not as a moderator).

Although LinkedIn is not primarily a social networking site employees should apply the principles set down within this policy to their use of this and similar professional networks.

### Guidance

- If you already make reference to your employment at the school on a personal internet site as defined above, or you intend to create such a site, you should inform your Headteacher.
- If you do refer to your employment at the school you must use a disclaimer such as "the views contained in these web pages are my personal views and do not represent the views of the School".
- Do not use the school logo on any personal web pages.
- Please be aware that using material from any copyrighted source without permission is likely to breach copyright.
- Carefully avoid bringing the school or its employees into disrepute and consult your Headteacher if you are unsure whether the content is appropriate.
- The school reserves the right to require removal of any material published by an employee which may adversely affect the school’s reputation or create risk of legal proceedings against the school.
- Do not reveal information which is confidential to the school - consult your Headteacher if you are unsure.
- Do not include or use any school, data, information, contact details or photographs of employees, pupils, parents or partner organisations without the explicit written permission of the school and the explicit written permission of the data subject (e.g. person shown in any photograph).
- Do not include comments or photographs which could bring into question your professional credibility.
- Time spent accessing social networking sites at work, for personal use, using school equipment must comply with the IT Policy applicable within the school. This includes the use of school equipment at home such as smart phones, tablets or laptops whether during or outside working hours.
- Do not invite or accept as ‘friends’ on such sites any child or vulnerable adult or the family members of any child or vulnerable adult you have met in the course of your employment.
- If you receive press or media contact regarding the content of your personal site and feel there may be implications for you or which in any way relates to the school, you should consult your Headteacher.

## Policy Decisions

### Authorising internet access

- All staff must read and sign the “Staff code of conduct” and read the “Social networking policy for school staff” and “E-safety policy” before using any school ICT source.
- The school maintains a record of all staff and children who have access to the school’s ICT systems.
- Parents are asked to sign a consent form regarding their child’s internet use (see Computer and Internet Agreement).

### Assessing risks

- The school takes 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 computer connected to the school network.
- Neither the school, nor Armstrong Bell can accept liability for any material accessed, or any consequences of internet access.
- The school’s e-safety policy and its implementation will be monitored and reviewed on a regular basis.

### Employee privacy and dignity

- Employees are strongly recommended to check that their online privacy settings only allow “friends” to see their profiles and that the privacy settings of “friends” do not inadvertently allow access to the employee’s own profile. It is also advised that as a general measure to protect their personal safety and identity, staff do not accept friend requests from people who are not personally known to them.
- Employees may wish to ask friends to check before photographs are posted which may cause them embarrassment. Employees posting their own images should bear in mind the fact that any image can easily be downloaded and manipulated and they should choose which images they share accordingly.
- It is recommended that employees do not post images that could be used to identify their homes or families.

### Compliance

- The School reserves the right to take action under the Disciplinary Policy should employees breach this policy or bring the school into disrepute by their actions on the internet.
- Employees must ensure that their use of social networking sites does not breach the Safeguarding Policy or Code of conduct.

### Handling e-safety complaints

- Complaints of internet misuse by children must be referred to the Computing Subject Leader in the first instance.
- Any complaint about staff misuse must be referred to the Head of School or Deputy Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the school’s child protection policy. The Designated Leader Team should be notified immediately.
- Pupils and parents are informed of the complaints procedure.

- Pupils and parents are informed of the consequences for pupil misuse of the internet (see Computer and Internet Agreement).

## Communications Policy

### Introducing the e-safety policy to pupils

- The schools E-safety rules are displayed on every netbook trolley and in various areas of the school so all users can see them.
- Pupils are informed that network and internet use is monitored and appropriately followed up.
- The children receive e-safety lessons and are constantly reminded of online safety.

### Staff and the e-safety policy

- All staff are trained regularly and receive a copy of the e-safety policy.
- Staff are informed that network and internet traffic can be traced to an individual user.

### Enlisting parents' and carers' support

- Parents’ and carers’ attention is drawn to the school’s E-safety Policy in newsletters, the school brochure and on the school website.
- The school asks all new parents to sign the pupil/parent agreement when they register their child with the school.