Inspire Care Achieve

# Computing & E-Safety Policy

Our e-safety policy has been written by the school, building on the NGfL policy and government guidance.

*The School e-Safety Coordinator:* ***Mr N Moore***
*The School Newtork Manager:* ***Mr J Gardner***
*The School ICT Manager:* ***Mrs A Gent-Jones***

*The date for the next policy review is* ***January 2018***

"The Governors of Greenbank High School are committed to safeguarding and promoting the welfare of children and young people at every opportunity and expect all staff and volunteers to share this commitment"

## Rationale

The Internet offers great experiences for adults and children. There are opportunities to improve your life, enhance your education or pursue business interests. Nowadays, young people are often enthusiastic Internet users - particularly of interactive services like: Email, Chat and Instant Messaging. However, like many exciting activities, there are risky situations to deal with and hazards to avoid.

## Why is internet use important?

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

## Internet Access

If staff or pupils discover an unsuitable site, it must be reported to the ICT Manager. Children will only be able to access the internet (at school) when under adult supervision. Internet access will be planned to enrich and extend learning activities. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, evaluation and retrieval.

Teachers should ensure that the use of internet derived complies with copyright law.

## How will information systems security be maintained?

The security of the school information systems and users will be reviewed regularly.

- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may be used without specific permission.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network maybe subject to inspection.
- The Network Manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced. This will be reviewed regularly and staff who have left will be blocked from accessing the system.
- All computer activity on school owned devices may be monitored and, where appropriate, screen captures taken when suspicious activity is detected. This is in addition to internet filtering as described below.

## How will email be managed?

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a member of staff if they receive offensive email. In the first instance this will be the class teacher.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- The forwarding of chain messages is not permitted.
- Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use personal email accounts during school hours or for professional purposes.

## How will published content be managed?

- Images or videos that include pupils will be selected carefully and will not provide material that could be abused.
- 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 images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or their parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

## How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. This topic will be covered in e-safety lessons and assemblies.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff must obtain written consent from the Headteacher or Deputy Headteacher before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website or VLE. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites. This should also be reported to the Child Protection Lead: Mrs E Russell (Assistant Headteacher for Pastoral Care)
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in Appendix 1 "Responsible Internet Use"

## How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school has a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) should report any breaches to the e-Safety Coordinator or Network Manager.
- If staff or pupils discover unsuitable sites, the URL will be reported to the e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Metropolitan Police or CEOP
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

## School Website

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or students' home information will not be published.
- Website photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' 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 students are published on the school Website.

## How will emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the terms set down in this policy.

## How should personal data be protected?

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

## How will the risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Metropolitan Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

## How will mobile phones and personal devices be managed?

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. If there is suspicion that the material on the mobile may

provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used during the school day including when pupils come on site before school.
- Filtered WiFi access is available to all school staff, and for pupils where specific permission has been granted by the Senior Leadership Team.

## Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the Headteacher's office. Mobile phones and devices will be released to pupils or parents/carers in accordance with the school policy.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

## Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will have access to a school phone where contact with pupils or parents/carers are required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- Staff must not use personal devices such as mobile phones or cameras to take photos or videos of pupils.
- If a member of staff breaches the school policy then disciplinary action may be taken.

**Appendices**

1) Responsible Internet Use: Rules for Staff.
2) Responsible Internet Use: Rules for Pupils.
3) Consent Form.

*Appendix 1*

Inspire Care Achieve

# Responsible Staff Computer / Internet Use

The computer system is owned by the school. This Responsible Internet Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made
- Anonymous messages and chain letters are not permitted.
- The uses of personal mobile devices during lessons are not permitted, unless agreed by the Senior Leadership Team for a specific purpose.
- The school ICT systems may not be used for private purposes, unless the headteacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted.
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

| | |
|---|---|
| **Name** | |
| **Signature** | |
| **Date** | |

***Appendix 2***

Inspire Care Achieve

# Responsible Pupil Computer / Internet Use

The computer system is owned by the school. This Responsible Internet Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of your Internet access.
- Computer access must be made via your own account and password, which must not be given to any other pupil.
- You must not attempt to load software or music onto the school computers.
- You must not search for inappropriate material that other people could find offensive.
- School computer and Internet use must be appropriate to your education.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by your teachers.
- You must never publish information about yourself or any person know.
- You are responsible for all e-mail you send and for contacts made.
- Anonymous messages and chain letters are not allowed.
- The uses of personal mobile devices during lessons are not permitted, unless agreed by your teacher for a specific purpose.
- You must not share images or video of yourself or other pupils with anybody else.
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

The school will monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

| | |
|---|---|
| **Name** | |
| **Signature** | |
| **Date** | |

*Appendix 3*

Inspire Care Achieve

# Consent Form
## Responsible Computer / Internet Use

Please complete, sign and return to the school

***Student:*** _____ ***Form:*** _____

### Student's Agreement

I have read and I understand the guidance for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

***Signed:*** _____ ***Date:*** _____

### Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

***Signed:*** _____ ***Date:*** _____

***Please print name:*** _____

### Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my daughter's work may be published on the school website. **Yes / No**

I agree that photographs that include my daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used. **Yes / No**

***Signed:*** _____ ***Date:*** _____