



Hemingford Grey
SCHOOL

Electronic Communication E-Safety Policy*

***Incorporating The School Digital Charter for KS1 & KS2
Acceptable Use Policy (AUP) - Appendix 1-3**

Date policy reviewed and approved: January 2020
--

**For the school's policy on use of social media and staff E-safety AUP,
please refer to the separate Electronic Communication Policies.**

HEMINGFORD GREY PRIMARY SCHOOL

E-SAFETY POLICY

1 Introduction

The requirement of this policy is to ensure that children learn to use the internet and related communications technologies appropriately and safely.

The range of hardware, networking systems and interactive sites is constantly expanding and the scope of this policy must develop accordingly, so that it goes beyond computers and the Internet to cover increasingly sophisticated equipment, including mobile phones, digital cameras, games consoles and communications platforms, including texting, interactive gaming and social networking.

The school is fully committed to encouraging pupils to use the exciting and innovative new technological tools in school and at home to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of or inappropriate sharing of personal information
- The risk of being subject to grooming by those with whom they make contact
- The distribution of personal images and information without an individual's consent or knowledge
- Inappropriate communication and contact with others, including strangers
- Cyber-bullying

It has been approved by governors, and will be reviewed annually.

The policy outlines what the school believes are the most appropriate ways for pupils and staff to use computers, the Internet and related communications technologies safely and appropriately.

It explains how we strive to meet legal and moral responsibilities.

2 Aims and Values

Our aim is to produce learners who are safe, confident and effective users of ICT. We aim to meet the requirements of the National Curriculum, offering opportunities for pupils to evaluate the use and impact of ICT in their learning.

We encourage individual achievement alongside consideration for the needs of others. We promote this through the Acceptable Use Policy and the Schools Digital Charter which are signed by the class annually and on display in each classroom and is discussed at an appropriate level with each class.

See Appendix 1 & 2- Digital charter for KS1 and KS2.

3 Online Work

Internet access raises educational standards by creating valuable opportunities to extend the range of information, resources and people which children can encounter, e.g. museums, art galleries, world wide educational resources, cultural and information exchanges between students world-wide.

It supports the professional work of staff and enhances the school's management of information and business administration systems, e.g. access to educational materials and good curriculum practice.

Guided experience in the use of ICT will encourage its safe use inside and outside school across an expanding range of devices, platforms and programmes.

3.1 Internet Access

Internet access will provide effective learning for children by:

- teachers setting clear objectives for internet use;
- teachers selecting and supervising access to sites which will support the learning outcomes planned for pupils' age and maturity;
- filtering appropriate to primary age pupils through the ICT provider;
- pupils being educated in taking responsibility for their own internet access;
- staff 'bookmarking' approved sites

3.2 Assessing Internet Content

At an appropriate age, children will be:

- taught ways to validate information before accepting that it is necessarily accurate
- encouraged to tell a member of staff immediately if they encounter any material which makes them feel uncomfortable
- taught to acknowledge sources of material used in their work as appropriate

3.3 E-mail, Blogs and Social Networking

E-mail and interactive websites provide opportunities to communicate quickly and effectively with a wide range of people and places which have otherwise been beyond the reach of pupils.

In addition:

- incoming mail will be monitored by the school and LA
- the forwarding of chain letters is not permitted
- children will not be allowed access to public chat rooms or networking sites including Facebook, Instagram etc.
- Individuals will take suitable measures to ensure that sensitive and confidential material is protected from third party viewing

3.4 Web Publishing

When publishing material on the world-wide web:

- the Headteacher will delegate editorial responsibility to a staff member to ensure that content is accurate and quality of presentation is maintained;
- the point of contact on the web site should be the school address and telephone number - home information or individual e-mail identities will not be published;
- first names only will be used on the web site – parents may request that a pseudonym be used where a pupil is at risk of identification through their first name, or that their name not be used at all
- no photographs of pupils will be used without parental permission

3.5 Staff Internet Use

Please refer to the Electronic Communication Staff E-Safety Acceptable Use Policy and the Social Media Policy.

3.6 New Devices and Applications

New devices and applications are being developed all the time; however, most begin without the needs of young users and their security being considered, therefore new applications will be thoroughly tested before pupils are given access to them in school. Pupils' mobile phones and other portable devices are excluded from school. However the school recognises that pupils are increasingly exposed to new technology outside school and the safe use of all available technologies inside and outside school will be encouraged in school.

4 Internet Safety

Internet access is a necessary part of the statutory curriculum. It is an entitlement for pupils based on responsible use. Parents and carers are kept up to date with relevant safety advice.

4.1 Range of Access

Pupil internet access will reflect the age and maturity of children in line with curriculum expectations.

4.2 Unsuitable Content

In common with other media, some material available online is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that they access only appropriate material. The school's ICT providers will see that checks are made to ensure that the filtering methods selected are effective.

However, due to the international scale and linked nature of information available via the Internet, it is not possible to totally guarantee that unsuitable material will never appear on a terminal. Neither the school nor Cambridgeshire County Council can accept liability for the material accessed, or any consequences thereof.

The use of computers without permission and for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks include the school has provided enhanced user-level filtering through the use of the filtering programmes. Staff are able to make requests for sites to be added or removed from the filtered list, which will be considered by the Network Manager and The ICT Service.

The school will monitor the effectiveness of strategies and systems to review and minimise risks through use of the AUP and teachers will give pupils clear guidance about internet access. Any e-safety incidents or concerns will be reported to a DSL and where appropriate the ICT provider.

Staff, parents and governors will work to establish agreement that every reasonable measure is being taken.

The school will work in partnership with the LA, DfEE, Internet Service Provider and parents, to ensure systems which protect pupils are reviewed and improved.

5 Legal Issues

Pupils, staff and parents are expected to observe copyright regulations in respect of photocopy and electronic copying. We insist that all software used in school is suitably licensed and this is monitored annually. In addition:

- security strategies will be discussed with the LA
- virus protection is installed and updated regularly

- third party software should not be used on school computers unless in agreement with the ICT strategic team

6 Complaints

Responsibility for handling incidents will be given to members of the Senior Management Team. Parents and pupils will need to work in partnership with staff to resolve any such issues.

7 Monitoring and Review

The ICT strategic team and the Head Teacher are responsible for checking that the policy is being implemented on a day-to-day basis, and for discussing its effectiveness regularly.


This policy will be reviewed annually as part of the Governors' usual review cycle.

8 School Website


Children's safety has to be paramount and this policy is intended to ensure that the school website does not expose children to danger or abuse by publishing personal information about them that could be misused in any way.

The following will be implemented:

- We will protect the identity of young people: we will not publish personal information (phone numbers, e-mail addresses) and we will only publish photos of children with written parents'/carers' permission. Photos of children will not include children's names unless used for a specific purpose and in these cases we will seek permission to publish the child's photo and his or her name.
- We will only publish personal information about adults if there is a valid reason to do so **and** we have obtained their explicit consent.
- We will not provide links directly to children's sites or email addresses from web pages.
- We will nominate a senior member of staff to be responsible for the site overall, checking legal issues, obtaining parents'/carers' permission to include children's work and ensuring that it presents the school correctly.
- We will nominate a website editor to check on a regular basis that links work and to remove or archive out-of-date material.



HEMINGFORD GREY SCHOOL DIGITAL CHARTER



Your Digital Rights

You have the **right** to work with a range of technology including: iPads, laptops, clever touch boards and PCs.

You have the **right** to access your class blog and Edmodo page to help with your learning both in school and out of school.

You have the **right** to explore the internet but remember you can't believe everything that you find on the internet.

You have the **right** to say when your photograph is used online.

You have the **right** to be safe online.

You have the **right** to tell an adult if you see something you don't like. You won't get into trouble.

You have the **right** to be treated with respect online.. Nobody should say anything to upset you!

Your Digital Responsibilities

I **will** only use the internet when I am around adults who can make sure I am safe.

I **will** keep my personal information private when I'm online.

I **will** only send polite and friendly messages online.

I **will** only click on links I know are safe. If I'm not sure I will ask an adult.

I **will** only go onto websites and apps an adult has said are safe to use.

I **will** only talk to people online I know or an adult has said it is OK to talk to.

If I see something online I don't like I **will** always tell an adult.

I know my digital rights and responsibilities..

Resourceful


Resilient

Risk takers

Relationships


Respectful

Reflective



HEMINGFORD GREY SCHOOL

HEMINGFORD GREY SCHOOL DIGITAL CHARTER



HEMINGFORD GREY SCHOOL

Your Digital Rights

You have the **right** to explore the Internet but you know that you cannot trust everything you see or read.

You have the **right to not** be videoed or photographed by anyone else and for those pictures **not** to be shared without your permission.

If you accidentally see something you don't like on the internet you have the **right** to tell someone and not feel guilty or get into trouble..

You have the **right** to be treated with respect.

You have the **right** to stay safe online and the **right** to tell an adult if someone is bullying you or being unkind to you online.

You have the **right** to access your class blog and Edmodo page to help with your learning both in school and out of school.

You have the **right** to know who you are talking to online and you don't have to talk to someone if you don't want to.

You have the **right to not** be judged by others when you report something that makes you feel uncomfortable or violates your privacy.

You have the **right** to keep your personal information private.

Your Digital Responsibilities

It is your **responsibility** to remember that not everyone is who they say they are online.

It is your **responsibility** to never arrange to meet someone you have only met on the internet unless your parent/ carer has given permission and you take a responsible adult with you.

It is your **responsibility** to only use school technology for school work and home work.

It is your **responsibility** to not give out any personal information that can be used to identify you, your family or friends, including: addresses, phone numbers, surnames and birth date.

It is your **responsibility** to only edit or delete your own work and not look at or change other peoples work without their permission.

It is your **responsibility** to report any unsuitable material you accidentally come across online or that is sent to you.

It is your **responsibility** to treat others with respect when online and you should not use language to upset others.

I am aware that some websites have age restrictions and it is your **responsibility** to respect this.

It is your **responsibility** to only send or upload information that is polite and sensible.

It is your **responsibility** to only contact or message people that you know unless it has been approved by an adult.

It is your **responsibility** to only open attachments or files from people you trust.

Resourceful

Resilient

Risk takers

Relationships

Respectful

Reflective