



Hemingford Grey
SCHOOL

Electronic Communication Staff E-Safety Acceptable Use Policy

*** Incorporating the E-Safety incident report form, School Digital
Charters (See Appendices 1-3)**

Date policy was last reviewed and approved:	April 2019
--	-------------------

Hemingford Grey Primary School

This policy covers the following aspects of e-safety in relation to all school staff:

- **Use of school based equipment**
- **Social Networking**
- **Managing digital content**
- **Email**
- **Mobile phones and devices**
- **Learning and teaching**

All staff should read and sign this document to demonstrate that they agree with the statements.

School Based Equipment

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the ICT Support Assistant.
- All passwords I create will be in accordance with the school e-safety Policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems.
- I will not share my passwords.
- I will seek consent from the Headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the Headteacher.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Headteacher.

- I understand my personal responsibilities in relation to the [Data Protection Act](#) and GDPR March 2018 the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- I will only use school-owned or provided portable storage (USB sticks, SSD cards, portable hard drives etc).
- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.
- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example spread sheets/other documents created from information located within the school information management system).
- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the Headteacher.
- I understand that 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 the appropriate authorities.
- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.

Social Networking

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any social media tools to communicate with parents unless approved in writing by the Headteacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- Staff must not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the ICT Support Assistant / Headteacher.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the e-safety Policy/ Home School Agreement (or any other relevant policy).
- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from a member of the Senior Leadership Team.
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any [copyright licencing](#).
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and deleted as soon as possible from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Email

- I will use my school email address for all correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will seek permission if I need to synchronise any school email account with a personally-owned handheld device.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- Emails sent to external organisations will be written carefully and if necessary authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the Headteacher, line manager or another suitable member of staff into the email.
- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode during school hours.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- I will not contact any parents or pupils on my personally-owned device.
- I will not use any personally-owned mobile device to take images, video or sound recordings.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach age appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

.....

Agreement

I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.

I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Name :
Role in School:
Signed
Date:
Accepted by:
Date:

Appendix 1

E-safety incident report form



School/organisation's details:

Name of school/organisation: Hemingford Grey Primary School

Address: St Ives Road, Hemingford Grey, St Ives, Huntingdon, PE28 9DU

Name of e-safety contact officer: Sarah Askew

Contact details: saskew@hemingfordgrey.cambs.sch.uk

Tel: 01480 375040

Details of incident

Date happened:

Time:

Name of person reporting incident:

Where did the incident occur?

☐ In school/service setting ☐ Outside school/service setting

Who was involved in the incident?

☐ child/young person ☐ staff member ☐ other (please specify)

Type of incident:

- ☐ bullying or harassment (cyber bullying)
- ☐ deliberately bypassing security or access
- ☐ hacking or virus propagation
- ☐ racist, sexist, homophobic religious hate material
- ☐ terrorist material
- ☐ drug/bomb making material
- ☐ child abuse images
- ☐ on-line gambling
- ☐ soft core pornographic material
- ☐ illegal hard core pornographic material
- ☐ other (please specify)

Description of incident

Nature of incident

☐ **Deliberate access**

Did the incident involve material being;

☒ created ☐ viewed ☐ printed ☐ shown to others

☐ transmitted to others ☐ distributed

Could the incident be considered as;

☒ harassment ☐ grooming ☐ cyber bullying ☐ breach of AUP

☐ **Accidental access**

Did the incident involve material being;

☐ created ☐ viewed ☐ printed ☐ shown to others

☐ transmitted to others ☐ distributed

Action taken

☐ **Staff**


- ☐ incident reported to Headteacher/Senior Leader
- ☐ advice sought from Safeguarding and Social Care
- ☐ referral made to Safeguarding and Social Care
- ☐ incident reported to police
- ☐ incident reported to Internet Watch Foundation
- ☐ incident reported to IT
- ☐ disciplinary action to be taken
- ☐ e-safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)


☐ **Child/young person**

- ☐ incident reported to Headteacher/Senior Leader
- ☐ advice sought from Safeguarding and Social Care
- ☐ referral made to Safeguarding and Social Care
- ☐ incident reported to police
- ☐ incident reported to social networking site
- ☐ incident reported to IT
- ☐ child's parents informed
- ☐ disciplinary action to be taken
- ☐ child/young person debriefed
- ☐ e-safety policy to be reviewed/amended

Outcome of incident/investigation



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 tell an adult if you see something you don't like. You won't get into trouble.

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

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 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.

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

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

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

I know my digital rights and responsibilities..

Resourceful


Resilient

Risk takers


Relationships

Respectful

Reflective



HEMINGFORD GREY SCHOOL DIGITAL CHARTER



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