Heavers Farm and Selsdon Primary Schools
Esafety, Acceptable Use and Camera and Image Policy 2016/17

ONLINE SAFETY

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation; technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful material
- **contact:** being subjected to harmful online interaction with other users
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm

FILTERS AND MONITORING

Both schools have an appropriate filtering and monitoring system in place. Children are asked to hand their mobile phones into the school office at the start of the school day and they are handed back at the end of the day.

THE PREVENT DUTY AND E-SAFETY

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well being of any pupil is being compromised.

PUBLISHED CONTENT AND THE SCHOOL BLOGS

The contact details on the blogs should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

The Executive Headteacher, Head of School or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

PUBLISHING PUPILS' IMAGES AND WORK

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the blogs, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school blogs.

INFORMATION SYSTEM SECURITY

- School IT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

PROTECTING PERSONAL DATA

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

This policy complies with the requirements of the Data Protection Act 1998, Freedom of Information Act 2000, Human Rights Act 1998 and other relevant Acts regarding the taking and use of photographic images of children.

All images will be used in a manner respectful of the eight Data Protection Principles. This means that images will be:

- Fairly and lawfully processed
- Processed for limited, specifically stated purposes only
- Used in a way that is adequate, relevant and not excessive
- Accurate and up to date
- Kept on file for no longer than is necessary
- Processed in line with an individual's legal rights
- Kept securely
- Adequately protected if transferred to other countries.

Where necessary, registration as a data controller will be applied for to allow personal information to be processed.

ASSESSING RISKS

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The schools will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

HANDLING E-SAFETY COMPLAINTS

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance
- with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to
- establish procedures for handling potentially illegal issues.

CAMERA USE AND IMAGES

The use of cameras on mobile phones is an essential and integral part of everyday life. As such, children and young people and early years practitioners and their managers are to be encouraged to use such technology in a positive and responsible way.

It has to be recognised however, that digital technology has increased the potential for cameras and images to be misused and inevitably there will be concerns about the risks to which children and young people may be exposed.

We recognise that having the right policies and practices in place will also protect school staff from misunderstanding, false accusations and damage to reputation around the use of digital images. Practical steps must be taken to ensure that the use of cameras and images will be managed sensitively and respectfully. A proactive and protective ethos is to be reflected which will aim to promote effective safeguarding practice.

It must, however, be acknowledged that technology itself will not present the greatest risks, but the behaviours of individuals using such equipment will.

We aim to ensure safer and appropriate use of cameras and images through agreed acceptable use procedures. This is to be in line with legislative requirements and will aim to respect the rights of all individuals.

Our policy will apply to all individuals who are to have access to and/or be users of work-related photographic equipment. This will include children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

This policy will apply to the use of any photographic equipment. This will include mobile phones, video cameras, webcams and portable gaming devices with inbuilt cameras as well as other forms of digital technology and resources for storing and printing images.

The Senior Safeguarding Officer is to be responsible for ensuring the acceptable, safe use and storage of all camera technology and images. This will include the management, implementation, monitoring and review of the Camera and Image Policy.

At our schools all staff and parents/carers are required to sign the appropriate Acceptable Use Policy. When taken together these cover the requirements of, and set out the procedures for, the taking and storage of photographs, digital images and videos.

Additionally, all parents/carers are asked to sign to give their consent to photographs, digital images and videos being taken and are made aware of the contexts, nature and the use to which these will be put.

The relevant Acceptable Use Policies are attached to this document.
Review date November 2017

Name of organisation	Heavers Farm and Selsdon Primary Schools
AUP review Date	November 2016
Date of next Review	November 2017
Who reviewed this AUP?	The Federated Governing Body of Heavers Farm and Selsdon Primary Schools

Acceptable Use Policy (AUP):
Adults working with children agreement form

This covers use of digital technologies in our school including email, Internet, intranet and network resources, learning platform, blogs, software, equipment and systems.

- I will only use our school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the school leadership team.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access any of our school systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with our school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that any / my personal online communication tools must not be used with service users and will not communicate or 'befriend' any service user using such methods.
- I will only use the approved email system for any email communication related to work at our school. This is currently teachers2parents or lgfl mail.
- I will only use other our school approved communication systems for any communication with young people or parents/carers. In this organisation the systems used are: the school blogs and/or Fronter.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / our school named contact. This is: Jeannette Brackenbury.(HF) or Stuart Woolley (SPS).
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.

- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using our school's recommended anti-virus, firewall and other IT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of young people or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role. I understand that it is my responsibility to ensure I know how to use any such tools so as not to compromise my professional role, such as setting appropriate security settings.
- I will not create a business account on any social networking site unless in full agreement with the appropriate manager, agreed for specific circumstances.
- I agree and accept that any computer, laptop or iPad loaned to me by our school is provided solely to support my professional responsibilities and that I will notify the them of any "significant personal use" as defined by HM Revenue & Customs.
- I will access our school resources remotely (such as from home) only through approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow our school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to service users, held within our school / LA's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand that it is my duty to support a whole organisation safeguarding approach and I will alert the our school's named child protection officer / relevant senior member of staff if I feel the behaviour of any service user or member of staff may be a cause for concern or inappropriate.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand our school's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use our school's IT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

Selsdon/Heavers Farm Primary School .....

Authorised Signature

I approve this user to be set-up.

Signature .....…… Date .....

Susan Papas – Executive Headteacher

e-safety agreement form: Parents

Parent / guardian name: ……..

Pupil name: …… Class ……

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, LGfL e-mail* and other IT facilities at school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email*, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / guardian signature:_____Date____/___/__

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the Esafety Policy. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature:_____Date____/___/__

Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

Only images of pupils in suitable dress will be used.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the staff or another child) as part of a learning activity; e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom or on the class blog.

- Your child's image for presentation purposes around the school; e.g. in school wall displays and presentations to capture images around the school or in the local area as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. a document sharing good practice; leaflets/banners advertising our school; in our school prospectus, on our school blog or on the class blogs.

- Your child could appear in the media if a newspaper photographer or television film crew attend an event. If this is the case then a separate consent form will be given to you in order for you to give permission.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Keeping safe: stop, think, before you click!
12 rules for responsible IT use

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for schoolwork and homework.
2. I will only edit or delete my own files and not look at, or change, other people's files without their permission.
3. I will keep my logins and passwords secret.
4. I will not bring files into school without permission or upload inappropriate material to my workspace.
5. I am aware that some websites and social networks have age restrictions and I should respect this.
6. I will not attempt to visit Internet sites that I know to be banned by the school.
7. I will only e-mail people I know, or a responsible adult has approved.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
10. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
11. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
12. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.