BELL FARM

PRIMARY SCHOOL

ICT AND ONLINE SAFETY POLICY

May 2017

Bell Farm Primary School

Online Safety policy

Online safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for **behaviour, safeguarding, anti-bullying and use of mobile phones and cameras in school.**

Using this policy

- The school's online safety co-ordinator is Helena Saunders.
- Our online safety policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The online policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The online safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff/pupil.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by **personal** passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The security of school IT systems will be reviewed regularly.
- **All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.**
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet Use

The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and pupils or families will take place using school equipment and/or school accounts.

Pupils will be advised not to give out personal details or information which may identify them or their location.

E-mail

- **Pupils and staff may only use approved e-mail accounts on the school IT systems.**
- Staff to pupil email communication must only take place via a school email address.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- **The school will consider how e-mail from pupils to external bodies is presented and controlled.**

Published content eg school website, school social media accounts

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreycc.gov.uk/?a=168635

Use of social media

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils and age restrictions should be adhered to.
- Pupils will be advised to use nicknames and avatars when using age appropriate social networking sites.
- If the school is made aware that children are using social networking sites while below the required age, they will inform the network provider to have that account deleted.

- Pupils should not attempt to contact members of staff via social media outside school.

Use of personal devices

- **Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the online safety policy and the relevant AUP.**
- **Staff must not store images of pupils or pupil personal data on personal devices.**
- **The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.**

Policy Decisions

Authorising access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the ‘Staff AUP’ before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- **At EYFS and Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.**
- **At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.**
- People not employed by the school must read and sign a Guest AUP before being given access to the internet via school equipment.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

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. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.

Handling online safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools’ behaviour policy.

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school online safety policy.

Communication of the Policy

To pupils

- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet
- Pupils will be reminded about the contents of the AUP as part of their online safety education

To staff

- All staff will be shown where to access the online safety policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet.
- All staff will receive online safety training on an annual basis.

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School online safety Policy in newsletters, the school brochure and on the school website.
- Parents will be offered online safety training annually

Source: Surrey County Council Online safety toolkit for schools June 2014

Status of Policy	**Date**
Authored by A Cooper	May 2016
Policy reviewed	May 2017
Agreed by Staff	May 2017
Agreed by Governors (C & L)	May 2017
Review	Annually May 2018

Appendix 1

Bell Farm Primary School

Staff, Governor and Visitor
Acceptable Use Agreement / ICT Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with Bell Farm Primary School's online safety coordinator.

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

- I will only use the school's email / internet / intranet and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I understand that I am responsible for all activity carried out under my username.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that all electronic communications with parents, pupils and staff, including email, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.

- I will only take images of pupils and/or staff for professional purposes in line with school policy. I will not distribute images outside the school network without the permission of the Headteacher.

- I will not install any hardware or software without the permission of the contractors covering the school's ICT.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- I will respect copyright and intellectual property rights.

- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Headteacher.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will report any incidents of concern regarding children's safety to the online safety Coordinator, the Designated Child Protection Officer or Headteacher.

- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serous infringements may be referred to the police.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name…………………………………………………………………………………… (Printed)

Job title……………………………………………………………………………………………

Signature……………………………………………… Date……………………

Appendix 2

Bell Farm Primary School

Parent/Carer consent form and Online safety Rules

All pupils use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the online safety Rules have been understood and agreed.

Parent / Carer name: …………………………………………………………………

Pupil name: ………..……………………………………………………………….

As the parent or legal guardian of the above pupil, I have read and understood the attached school online safety rules and grant permission for my daughter or son to have access to use the internet, school email system and other ICT facilities at school.

I know that my daughter or son has signed an online safety agreement form and that they have a copy of the school online safety rules. We have discussed this document and my daughter or son agrees to follow the online safety rules and to support the safe and responsible use of ICT at Bell Farm Primary 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 online safety skills to pupils.

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

I understand the school is not liable for any damages arising from my child’s use of the internet facilities.

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 online safety.

Parent/Guardian signature: …………………………………………………………..

Date...

Please complete, sign and return to the school secretary

Our 5 Golden Internet rules!

- We will only look at websites that are appropriate for children.
- If we see something we don't like, we will tell an adult.
- We will only log on to the computer with our own details.
- We will always keep our personal information safe by not sharing details about ourselves with anyone else online.
- We will only use kind language when communicating with people online.

Remember, your ICT use is being monitored!