BEAUFRONT FIRST SCHOOL

Nurturing Happiness, Achievement and Respect

E-SAFETY AND RESPONSIBLE USE POLICY

Version History

Version	date	Author/contributor	Date approved	Approved by.	Next review.
	Sept 2017	Louise Atkinson Jackie Hughes			
1	Oct 2017	All Beaufront staff.			
				Govs. 7.3.17	

1 RATIONALE

1.1 E-Safety Policy
E-Safety encompasses internet technologies and electronic communications such as mobile phones, tablets and laptops as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

1.2 This e-safety policy encompasses responsible use of school equipment and the need to raise awareness of the safety issues associated with electronic communications as a whole.

1.3 Beaufront First School's E-Safety Policy will operate in conjunction with the E-Safety and Responsible Use of the Internet in School documents and in the context of other policies including those for Pupil Behaviour, Bullying and Curriculum, and in conjunction with our ethos as a Rights Respecting School.

1.4 E-safety depends on effective practice at a number of levels:

- responsible ICT use and acceptable use by all staff and pupils; encouraged by explicit training and education;
- staff and pupils will be trained and educated on what action to take in the case of inappropriate sites or emails. Appendix 1 attached to this document details the Northumberland County Council procedures to be followed in the case of any incident;
- sound implementation of e-safety policy – discussed termly in staff meetings;
- safe and secure internet provision is provided by Northumberland Council;
- effective management of filtering by both the school and the internet provider. Future Cloud has been set up within the school on all desktops and laptops. This enables a key logging system that sends a report to PCE Future Cloud. This report can be seen by the designated personnel Eileen Daniel, Jackie Hughes and John Devlin. Any queries about the report are followed up and staff are involved when necessary.
- school iPads are part of Northumberland's Lightspeed filtering system;
- informing parents about e-safety measures taken in school to safeguard children;
- individual staff, visitor and student log-ins on all computers and iPads

- **2. Teaching and Learning**

2.1 Why internet use is important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as apart of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Internet use will enhance learning

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online

safety curriculum should be broad, relevant and provide progression in the following ways:

- The school internet access will be designed expressly for pupil use and will include appropriate filtering.
- A planned online safety curriculum is provided as part of Computing and PHSE.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Key online safety messages are reinforced during assemblies and as part of whole school events such as Safer Internet Day.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils will be supported in PHSE lessons to build resilience to radicalisation by understanding that some people have extreme and controversial views both online and offline.

2.3 Teaching and Support Staff are responsible for ensuring that:

- **They have an up to date awareness of online safety matters and of the current school e-safety policy and practices.**
- **They have read, understood and signed the Staff Acceptable Use Policy**
- **They report any suspected misuse or problem to the e-safety co-ordinator and headteacher.**
- **All digital communications with pupils/ parents/ carers should be on a professional level and in accordance with the Beaufront Acceptable Use Policy for staff.**
- **Staff should not download executable files or install programmes on school devices without permission in accordance with the Beaufront Acceptable Use Policy for staff.**
- **Personal data is not sent over the internet or taken off the school site unless safely encrypted or otherwise secured.**
- **Online safety issues are embedded in all aspects of the curriculum and other activities.**
- **Pupils understand and follow the Pupil Acceptable Use Policy**
- **They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where**

allowed) and implement current policies with regard to these devices.

- **In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.**

2.4 Pupils:

- **Are responsible for using the school internet technologies in accordance with the Beaufront E-Safety Rules for Pupils**

2.5 Education: Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers will be encouraged to support the school in promoting good online safety practice and to ensure that digital and video images taken at school events will not be shared on social media sites, without written permission from the child's parents/ carers.

- **Information will be provided to parents regarding the promotion of e-safety at home in the form of letters, leaflets, suggestions on where to access advice such as on websites and provision of seminars and workshops, and events such as Safer Internet Day.**

3. Managing Internet Access

3.1 Information system security

- The service level agreement regarding school computing systems, capacity and security will be reviewed annually by the governing body.
- Virus protection on curriculum computers will be checked regularly by the school's Computing technician.
- Security strategies will be followed and implemented in line with Northumberland County Council advice and policies.
- Policy Central Enterprise forensic software is installed on all computers and laptops.

3.2 Managing devices

School owned:

- school iPads are part of Northumberland's Lightspeed filtering system
- Installation of APPs and management of settings will be undertaken by the E-Safety lead and deputy or Northumberland ICT support through Northumberland's Mobile Device Management system.
- Images taken on school iPads should be deleted once they have been used / downloaded onto a staff password protected account.

Personal devices:

- Pupils will not be permitted to bring to school or use personal technology on the school's premises, e.g mobile phones.
- Staff and visitors should ensure that Bluetooth is turned off in personal devices while on school premises. Phones should not be used while children are present.
- Staff should only use personal mobile phones to contact school if there is a change of plan or an emergency whilst on a school trip.

3.2 Email and Messaging Services

- Pupils may only use approved e-mail accounts or messaging services as part of the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail or message. Pupils will be taught how to deal with an incident of this nature, as part of the e-safety curriculum.
- Incidents of cyber-bullying will be reported to the E-safety co-ordinator and headteacher. The subject of cyber-bullying will be addressed through PHSE lessons and the E-Safety curriculum.
- Pupils must not reveal personal details of themselves or others in e-mail communications, or arrange to meet anyone without specific permission. Pupils will be educated about possible dangers of releasing personal information.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

3.3 Published content and the school website

- The contact details on the web site should be the school address, email, and telephone number. Staff or pupils' personal information will not be published.
- Pupils' full names will not be used anywhere on the website.

3.4 Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be easily identified by name.
- Written permission from parents or carers will be obtained, when a child first attends the school, before photographs of pupils are published on the school website or in any other form of media. (Appendix 2)

3.5 Social networking and personal publishing

- Access to social networking sites is presently controlled by the filtering service provided by Northumberland County Council.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. This will be reinforced by explicit e-safety teaching in school.
- Parents or carers will be informed in writing at the beginning of each school year that photographs of pupils should not be posted on any publically accessible domain, for example social networking sites such as Facebook.

Social networking – staff guidance

- Staff are strongly advised, in their own interests, to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it.
- All staff also need to be aware that parents and pupils/students may carry out web and social network service searches to find on-line information about staff, for example; background, interests, career experiences and self-presentation. All staff are advised to ensure that information available publicly about them is accurate and appropriate.
- Staff must not use internet or web-based communication channels to send personal messages to a child/young person, or their parents. This includes online gaming.

- Staff should not have any secret social contact with children and young people or their parents, for example, using a pseudo name on a social networking site.
- Staff must not give their personal contact details to children or young people, including their parents. - Staff are to understand that some of their communications may be called into question and may need to be justified.
- Staff are advised not to have online communications with ex-students who have recently left the school and may have friends or family still within the school.
- Staff are strongly advised to ensure that they enable all privacy and security settings on their social networking accounts, including the prevention of messages being sent to them as a result of an internet search. This will prevent young people accessing and potentially misusing their personal information, or making inappropriate contact.

3.6 Writing and reviewing the e-safety policy

The designated safeguarding lead should be trained in Online safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:

- **Sharing of personal data**
- **Access to illegal/ inappropriate materials**
- **Inappropriate on-line contact with adults/ strangers**
- **Potential or actual incidents of grooming**
- **Cyber-bullying**

- The school E-Safety co-ordinator is Louise Atkinson and the Deputy E-Safety is Jackie Hughes, our safety team includes Eileen Daniel (HT), Gemma Boucetla and Fran Booth. Eileen, Louise and Jackie receive and monitor weekly forensic software reports provided by Northumberland County Council about the use of the internet in school.
- This e-safety and responsible use policy has been written with current guidance in mind, particularly that provided by C.E.O.P. (The Child Exploitation and Online Protection Agency). Louise

Atkinson and Mrs Daniel are registered CEOP members. Louise Atkinson is also qualified as a C.E.O.P. ambassador.

- The e-safety policy and its implementation will be reviewed annually by the lead governor for Computing in conjunction with e-safety staff in school.
- The e-safety policy and its updates will be presented to and discussed by staff in staff meetings/ INSET days.
- "A Responsible Use of the Internet in School Contract and Rules for Pupils" document (Appendix 3) will be sent annually to parents for discussion with their child, signed and returned to school where it will be checked against the school role and filed.
- As part of their induction procedure, all staff, when beginning their employment at the school will sign an acceptable use contract and code of practice.

3.7 Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities as outlined in this policy.

- All staff will undertake NSPCC 'Keeping Children Safe Online' training.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Agreements.
- The e-safety co-ordinator will provide advice/training to individuals as required. e.g through Online Safety BOOST presentation resources (https://boost.swgfl.org.uk)

3.8 Training – Governors

The Governor responsible for Computing/ E-Safety will take part in online safety training/ awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by Northumberland County Council / National Governors association / or other relevant organisation.
- Participation in school training/ information sessions for staff or parents (this may include attendance at assemblies/ lessons)

September 2017

E-Safety Policy reviewed September 2017		
Date	**Shared with Staff**	**Shared with Parents**
	Eileen Daniel	
	Ben Hulbert	
	Jackie Hughes	
	Be Hulbert	
	Roz McCall	
	Louise Atkinson	
	Angela Mole	
	Gemma Boucetla	
	Grace Beresford	
	June Blaylock	
	Shirley Byerley	
	Liza Hamer	
	Fran Booth	