E-safety including Acceptable Use Policy

Formally adopted by the Governing Board/ Trust of:	**Bressingham Primary School**
On:-	**10.21**
Chair of Governors/Trustees:-	
Last updated:-	

Group:	Finance	DOCUMENT DETAILS		*Scope*:	Bressingham
Date of Last Review:	December 2021	*Next Review Date:*	**October 2023**	*Reviewing Body:*	**Full Governing Body**

Contents

1. Introduction and Overview

1.1. Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Bressingham Primary School with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

The main areas of risk for our school community can be summarised as follows:

Content
- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact
- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct
- Aggressive behaviours (including bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

1.2 Handling Concerns

Issues relating to the online safety of children and/or staff will be treated as any other safeguarding concern is dealt with in accordance with the Safeguarding Policy.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE)
- Staff and pupils are given information about infringements in use and possible sanctions
- Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not
- Support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- We will immediately refer any suspected illegal material to the appropriate authorities

2. Education and Curriculum

2.1 Pupil online safety curriculum

The use of computing equipment and the internet is taught through our Computing curriculum, RSHE and cross curricular sessions. It is very important that regulations and boundaries are in place for pupils and staff but also allowing pupils to be educated to take a responsible approach themselves. Therefore, in our schools, we:

- have a progressive online safety education programme as part of the Computing and RSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience,
- will remind pupils about their responsibilities; pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- ensure staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright,
- ensure that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.

2.2 Staff and governor training

It is recognised that for our staff to be good role models to the children in this school that they themselves will need to have a good knowledge of the computing and online safety curriculum.

This school makes regular up to date training available to staff on online safety issues (including CEOP) and the school's online safety education program as well as providing all staff with information and guidance on this Policy including training on section 6: Acceptable use of ICT and Social Media.

2.3 Parent/Carer awareness and training

This school:
• provides information for parents/carers for online safety on the school website
• runs online safety advice, guidance and training for parents - through information and links to appropriate content to support parents at home with staying safe online, together with training sessions

3. Managing the IT infrastructure

3.1 Internet access, security and filtering

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance. Occasionally, the protection mechanisms provided by the ISP provider fail, either because the offending web site is new and is not known by the protection mechanism, or because the mechanism itself has developed a fault. As a school we alleviate this problem by ensuring our pupils are monitored during internet activities and constantly maintain vigilance. Pupils are not allowed on the internet or email facilities without adult supervision.

Children and staff must make careful and considerate use of the school's ICT resources, report faults and work in a way that minimises the risk of introducing computer viruses to the system

All users are expected to act in a responsible, ethical and lawful manner. Users should uphold privacy and confidentiality in conjunction with the data protection policy and GDPR recommendations.

Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else. No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.

Users must not upload or download software on any device without the authorisation of the Headteacher.

Users must take care to store sensitive information, e.g. pupil data safely and to keep it password protected–preferably on cloud storage.

3.2 E-mail

At Bressingham Primary School:

- We provide staff and all children with an email account for their professional/educational use only.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of a school closure where home learning is in place, the parents of children, or children in Years 5 and 6, may use their email addresses to contact their class teacher (on a class email address) to share their work and learning. The content of these emails should be respectful and be fairly formal in style, as appropriate to a school setting. There may be times where teachers and staff use Microsoft Teams to conduct short video calls with the class as a whole. 1:1 video meeting should only happen where this has been arranged in advance and with appropriate parent/ carer permission. Staff would almost always make these calls from a school setting, and another member of staff should be able to overhear or oversee the meeting. When staff have to make video calls from a setting other than school, they are reminded to always remain professional during these meetings and therefore thinking carefully about the background of their video call etc.
- The official school email service is regarded as safe and secure and is monitored and is the only email address which should be used to contact parents.
- Any digital communication between staff and pupils or parents / carers (email, social media, etc.) must be professional in tone and content.

3.3 School website

- The school website complies with statutory DfE requirements
- Most material is the school’s own work; where other’s work is published or linked to, we credit the sources used and state clearly the author's identity or status
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with GDPR with regards the use of such images
- Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or on other platforms.

4. Digital Content

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet.

4.1 Digital images and video

In this school:

We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school.

We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils and parents/ carers must not take, use, share, publish or distribute images of others without their permission, *although parents and others attending organisation events are allowed to take photographs and videos of those events for domestic purposes, unless specifically asked not to. (Please see our Data Protection Policy for further information.)*

5. Acceptable use of ICT and Social Media

5.1 Mobile phone communication and instant messaging

- No children are allowed mobile phones in school.
- If a child requires a mobile phone before or after school the child may take the phone to the office to be securely locked away until the end of the school day.
- Staff are not to give their home telephone number or their mobile phone number to pupils.
- Staff are not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupils' text messages.
- Photographs and videos of pupils should not be taken with mobile phones, except the school mobile phone, for school purposes and after permission has been sought from the Headteacher; as soon as possible the images will then be transferred to the school system and deleted.
- Staff should not enter into instant messaging communications with pupils.
- Staff mobile phone communication should be used sparingly and only when necessary; children should not be present unless necessary. All staff are encouraged to leave mobile phones switched off in their bags which should be left in a classroom cupboard or other safe place during lesson times. If staff expect to receive a call during lesson time they should direct the caller to the school landline in the office. If/when the call is made the member of staff will be informed by the office and if necessary, given time to leave the classroom to return or take the call.

- The school permits the use of personal mobile phones on trips to contact the school if/when appropriate and necessary. The school does have its own mobile phone and this should be used in all out of school circumstances where possible.
- The use of mobile phones to record images from the visit is not permitted.

5.2 Social Media

Bressingham Primary School understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school. This school defines social media as any online platform that offers real-time interaction between the user and other individuals or groups including:

•Blogs
•Online discussion forums
•Collaborative spaces such as Facebook
•Media sharing services such as YouTube
•Micro-blogging applications such as Twitter

We would define ‘member of the school community’ as any teacher, member of support staff, pupil, parent/carer of a pupil, governor and member of the school kitchen staff.

Social media use –staff

•School social media passwords are kept in the office.
•The head teacher is responsible for the school’s social media accounts
•Staff must not access social media during lesson times unless it is related to the learning activity
•Staff may use social media during their break times but not in front of pupils.
•Members of staff must not ‘friend’ or otherwise contact pupils or parents through social media.
•If pupils or parents attempt to ‘friend’ members of staff through social media they should ignore requests.
•Members of staff should avoid identifying themselves as an employee of the school on social media.
•Members of staff must consider carefully the content of anything they post online and refrain from anything which is damaging to the school or any of its staff or pupils
•Where teachers or members of staff use social media in a personal capacity, they should make it clear that their views are personal. Staff may ‘like’ and ‘re-tweet’ but not tweet about the school from their personal account.
•Staff who also have links with parents should consider very carefully their use of any social media with due regard to those they are friends with, what they post. They should never make comments about the school or any staff or pupils. This will link to all the other points in this section.
•Teachers or members of staff must not post any information which could identify a pupil, class or the school.
•Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.
•Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.

•Members of staff should be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.
•Members of staff should regularly check their online presence for negative content via search engines.
•If inappropriate content is accessed online, an inappropriate website content report form should be completed and passed on to the Headteacher.
•Attempts to bully, coerce or manipulate members of the school community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter.
•Staff members should use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

Social media use –pupils and parents/carers

•Pupils should not access social media during lesson time as the school does not advocate the use of social media sites for children in the primary age range.
•Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.
•Pupils and parents/carers are requested not to attempt to “friend” or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they will be reported to the Headteacher.
•If members of staff attempt to “friend” or otherwise contact pupils or parents/carers through social media, they should be reported to the Headteacher.
•Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.
•Pupils and parents/carers must not post content online which is damaging to the school or any of its staff or pupils.
•Pupils at Bressingham Primary School should not sign up to social media sites that have an age restriction above the pupil’s age and parents/ carers should monitor this.
•If inappropriate content is accessed online on school premises, it must be reported to a teacher

Policies and documents to refer to:

- KCSiE (DfE)
- Teaching online safety in school (DfE)
- Guidance to Safer Working Practice
- Staff Code of Conduct

Group:	Finance	DOCUMENT DETAILS		*Scope*:	Bressingham
Date of Last Review:	December 2021	*Next Review Date:*	**October 2023**	*Reviewing Body:*	**Full Governing Body**