Brede Primary School

Policy name	On-line Safety Policy
Policy status	ESCC – statutory annual
Governing body reviewed	April 2019
Review date	April 2020

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Brede Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- 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.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Scope

This policy applies to all members of Brede Primary School community (including staff, pupils, volunteers, parents/carers, visitors, contractors and community users) who have access to and are users of Brede Primary school IT systems, both in and out of Brede Primary School. This policy covers personal use of social media as well as the use of social media for County Council work purposes, including sites hosted and maintained on behalf of the County Council. This policy applies to personal web space such as social networking sites, blogs, microblogs, chatrooms, forums, podcasts, open access online encyclopaedias, social bookmarking sites and content sharing sites. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

Roles and responsibilities

The Headteacher, has overall responsibility for online safety provision and is responsible for ensuring that all staff receives suitable training to carry out their safeguarding and online safety roles. The Headteacher also has overall responsibility for the school website and any other forms of communication relating to Brede Primary School. Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
In serious cases we will also take legal advice when dealing with any such misuse.
The Designated Safeguarding Lead, has day to day responsibility for online safety by promoting an awareness and commitment to online safety throughout the school

community. We ensure that online safety education is embedded within the curriculum and that all staff are aware of how to report online safety incidents.

The Governing Body will nominate a safeguarding governor and will ensure that the school has in place policies and practices to keep the children and staff safe online, approve the Online Safety Policy and review the effectiveness of the policy as well as supporting the school in encouraging parents and the wider community to become engaged in online safety activities. Governors should also take part in regular online safety training / awareness sessions.

The network technician will manage the school's computer systems, report any online safety related issues, regularly monitor the school's use of technology and ensure that appropriate back up procedures are in place as well as ensuring the network has up to date virus protection.

Teaching and support staff will embed online safety into the curriculum. They will supervise and guide pupils carefully when engaged in learning activities involving online technology. Staff should act as good role models in their use of digital technologies the internet and mobile devices.

All staff, volunteers, contractors and external groups will read, understand, sign and adhere to the school staff Acceptable Use Policy, have an up to date understanding of on-line safety matters (through a planned programme of formal online safety training) as well as modelling safe and responsible use of technology, reporting any suspected misuse to the Designated Safeguarding Lead. This will also form part of any induction processes.

Staff are responsible for ensuring that any mobile devices/ technologies loaned to them by the school, are used primarily to support their professional responsibilities. At the end of the period of employment/volunteering any equipment or devices loaned by the school will be returned. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Pupils are responsible for using the digital technology systems at Brede, in accordance with the Pupil Acceptable Use Agreement. They must understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. They should also know and understand policies on the taking / use of images and on cyber-bullying. Pupils should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that Brede's Online Safety Policy covers their actions out of school, if related to their membership of the school.

The school will seek to provide parents with information regarding online safety and awareness through curriculum activities, newsletters and parent evenings. Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required. We ask that they read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren. Parents need to ask permission before uploading photographs, videos or any other information about other people. We encourage parents to consult with the school if they have any concerns about their children's use of technology and to support the school in promoting online safety.

Education and Curriculum

We have a clear, set of online safety lessons as part of the Computing curriculum/PSHE and other curriculum areas as well as assemblies. This covers a range of skills and behaviours appropriate to their age and experience. We remind pupils about their responsibilities including how to save work and access work through the shared work area for pupils. We teach them about online safety paying particular attention to social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work. Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement, annually.

Expected Conduct

Mobile technology devices

Mobile technology devices might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. This is not an exclusive list and will include any new technologies that emerge.

Mobile technology devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices. No pupil should bring his or her mobile phone or personally-owned device into school, unless for a prior agreed curriculum use. Staff personal mobile devices will not be used during lessons. The use of school owned devices will not be used to harm/embarrass another person. They will not be used to bully or intimidate. Images, video and audio of pupils taken by staff will only be stored on school owned devices which remain on site. The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material. Devices containing photographs/ video should have them removed before the device is taken on a school trip.

Digital Communication

Any digital communication between staff and pupils or parents / carers (e.g. email, parent mail, social media, chat, blogs, website etc.) must be professional in tone and content.

Email

We provide staff with an email account for their professional use. The content of emails should not contain offensive content. Care should be taken when opening attachments unless from a trusted source. Offensive content should be reported to the Headteacher. Members of staff and pupils should not be discussed in emails unless using secure methods of communication.
Email should not be used to transfer staff or pupil personal data. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School Website

The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The school web site 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 web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Cloud Environments

Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas. Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community. In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social Media

It is expected that members of staff use social media responsibly so that confidentiality of personal and other sensitive information and East Sussex County Council's reputation are safeguarded. Staff must be conscious at all times of the need to keep their personal and professional lives separate.

Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- Human Rights Act 1998
- Common law duty of confidentiality
- GDPR May, 2018, and
- General Social Care Council Code of Practice for Social Care Workers.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. service user and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- County Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Incident Management

The school will take all reasonable precautions to ensure online safety; however it is recognised that staff may be able to access such sites by mistake when using search engines or when firewalls have not been able to prevent it. Where mistakes of this nature occur, staff must immediately notify the Headteacher or representative in writing. (See staff drive/welfare concern form). Where any content includes images of Child abuse then the matter should be referred to the Police immediately. Isolate the computer in question as any change to its state may hinder a later police investigation.

Inappropriate materials would cover any materials deemed unsuitable for staff to be accessing in relation to their post within school or working for the Local Education Authority. Examples of such materials are pornographic sites, on-line gambling, extreme political sites, discriminatory or illegal sites of any sort (e.g. sexist, ageist, homophobic, disablist, hate material that promotes violence or attack on individuals on the basis of religious, racial or gender grounds)

In fact all sites which conflict with the Council's equal opportunities policy) or sites which may produce a conflict of interest (e.g. signing petitions on line which are against school / Council policies/initiatives). This is a non-exhaustive list and should be used to guide staff when considering what sites to access.

There may be occasions when staff are required to access sites that contain otherwise inappropriate materials in order to carry out their professional duties as determined by the curriculum (e.g. accessing tabloid newspapers and articles about terrorism with regard to a media studies course). Permission should be sought from the Headteacher to search for such sites and, having accessed the sites, a record given of the material and sites which have been used.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003,
- Copyright, Designs and Patents Act 1988 and
- GDPR May, 2018

East Sussex County Council could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render the County Council liable to the injured party.

Review and Monitoring

This policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy and Anti-Bullying policy).

This policy will be reviewed annually.