

# Burlington Junior School

**Shaping Positive Futures**



**Achieving Our Full Potential**

## **E-Safety Policy**

Date adopted	25 <sup>th</sup> February 2021
Date approved by chair of Committee	25 <sup>th</sup> February 2021
Review date	25 <sup>th</sup> February 2022

At Burlington Junior School we believe that Computing is central to all aspects of learning; for adults and children in both the school and the wider community. Provision should reflect the rapid developments in technology.

Computing in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

We believe that E-Safety is the responsibility of the whole community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching whilst remaining safe when accessing these. Due to our whole school approach, we recognise that all members of our school and community have a responsibility in upholding and supporting safe practice in their classrooms and follow our E-Safety policies and procedures.

Computing leaders will remain consistently up to date with current guidance and issues through organisations such as East Riding Local Authority, Child Exploitation and Online Protection, Child Net and the UK Safer Internet Centre. Any alterations in legislation will then be discussed with the Head Teacher, Senior team and Governors when necessary.

Staff at Burlington Junior School have a good understanding of the school's policy including:

- Safe use of e-mail
- Safe use of the internet
- Safe use of the school network, equipment and data
- Safe use of digital images and technology, such as mobile phones and cameras
- Publication of pupil information/ photographs on the school websites

Once staff are aware of the policies and procedures in school they will then be required to sign our Acceptable User Policy (AUP) agreement to declare understanding of our protocol before using any technology in school (Appendix 1).

### **E-Safety in the curriculum**

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

- We will provide a series of specific E-Safety-related lessons in every Year group as part of the Computing and PSHE curriculum predominantly through Purple Mash.
- We will celebrate and promote E-Safety at a whole school level.

- We will educate pupils on the dangers of technologies that may be encountered outside school which is done informally when opportunities arise and as part of the curriculum.
- We will educate children about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the Computing curriculum.
- Pupils are taught awareness of the impact of online bullying through PSHE and are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.
- Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know
- We will discuss, remind or raise relevant E-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

#### **Using email and messaging facilities in education**

- Staff and pupils should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system can be monitored and checked.
- Pupils are introduced to email as part of the Computer Science Scheme of Work.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Staff and pupils are not permitted to access personal e-mail accounts during school.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.
- Class Dojo, Emails and text messages will be the main means of communication between staff and parents.

### **Using mobile phones**

- Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.
- Staff must not use their mobile phone in front of pupils unless in an emergency situation.
- Staff must not use their personal mobile phone to take or store photographs of pupils.
- If pupils bring mobile phones to school, they will be handed in at the school office at the start of the day.

### **Using new technologies**

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an E-Safety point of view.
- We will regularly amend the E-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an E-Safety risk.

### **Protecting personal data**

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission from the head teacher, and without ensuring such data is kept secure.
- Staff will use encrypted data storage for all school work on and off site.

### **Publishing pupil's images and work**

- On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:
- On the school web site
- In display material that may be used in the school's communal areas
- In display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)
- Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

### **Dealing with E-Safety incidents**

- Staff will log E-Safety incidents using CPOMS. The E-Safety coordinator or the Head teacher will be the first point of contact in school on all E-Safety matters.

## **Remote learning**

At Burlington Junior School during any partial or complete National lockdown forcing the closure of schools our remote learning will ensure that we stay connected as a school community. The learning provided will allow a continuation of learning and will deliver important support for pupil's well-being.

The platform that will be used for all remote learning sessions is Google Classroom, which is available through any device where Google is accessible. Information relating to any remote learning sessions including documents, video links and any other relevant material will be posted within Google Classroom. It is vital that children access Google Classroom every morning so that they can keep up to date with newly posted lessons and activities that they will be required to hand in.

In order to create a stimulating yet safe environment for our pupils, there are key areas which teachers must abide by:

- We must have consent from parents/ carers to access the remote sessions. (Appendix 3)
- Teachers must be familiar with the functions of Google Classroom including mute settings.
- Any remote sessions should be hosted and supervised by the class teacher.
- When using Google Meet, the pupils must exit first and the teacher should end the call to ensure unsupervised conversations do not occur.
- Teachers should ensure that during a Google Meet call they use an appropriate background as well as suitable clothing for both staff and pupils.

## **Filtering Internet access**

- The school uses a filtered Internet service. The filtering is provided through East Riding of Yorkshire Council, along with the Smoothwall filter.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the E-Safety coordinator.
- If users discover a website with potentially illegal content, this should be reported immediately to the E-Safety coordinator. The school will report this to appropriate agencies including the filtering provider, LA, Child Exploitation and Online Protection (CEOP).
- The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

## **Appendix 1**

### **Acceptable Use Policy for Pupils**

You can use the computers and other devices in school to access the Internet to help you with your learning. These rules will help make sure the Internet is a safe and fun place for everyone in school.

You will need to agree to follow these rules whenever you use ICT at school.

- I will ask permission from a member of staff before using the internet.
- I will only use the computers and other devices for school work and homework.
- I will not access files that belong to other people.
- I will only use equipment or files I bring from home, such as my mobile phone or files on a USB stick, if the school lets me, and for activities the school agrees to.
- I will only send messages to people I know, or my teacher has approved, as part of my lesson.
- The messages I send, and the work I do, will be polite and responsible, and will not contain anything that might upset someone else.
- I will only open attachments in messages I receive, or download a file, if I trust the person who sent it or the website it is from, and I've checked with my teacher that it is safe.
- I will keep my username and password safe by not telling anyone else.
- I will not change any settings on the computers and other devices I use at school.
- I will not install or delete any software on the computers and other devices I use at school.
- I will not give away any of my personal information, or the personal information of people I know, over the Internet. This includes my full name, address, phone numbers, photographs and videos of me and my friends, or the name of my school unless my teacher has checked it is safe.
- If something happens whilst using a computer or school device, and I am not sure what I should do next, I will ask a member of staff to help me.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- I understand that the school may check my computer files, the Internet sites I visit, the messages I send and anything else I do to make sure I am keeping myself and others safe.
- I understand that if I do not follow these rules and other guidance from the school as best as I can then I may not be allowed to use the Internet or any of the school's ICT equipment.

## **Appendix 2 Acceptable Use Policy for Staff and other adults in school**

These statements are designed to ensure staff and other adults in school are aware of their professional responsibilities when using the ICT systems provided. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and when using school ICT equipment at other locations such as your home.

- Any use of school ICT systems will be for professional purposes.
- Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using the ICT systems. You should not allow an unauthorised person to access the school ICT systems, e.g. by logging in for them.
- Any online activity should not harass, harm, offend or insult other users.
- You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should follow your school's procedure and report this immediately.
- You should not download or install any hardware or software without permission. If you have responsibility for installing software you should be confident it is adequately licensed and appropriate for educational use.
- Ensure that any files on removable media (e.g. USB drives, CDs) are free from viruses and other malware before use and that such devices are not used for carrying sensitive data or details of pupils, parents or other users without suitable security and without permission from the Headteacher.
- Any electronic communications should be related to schoolwork only, and should be through school e-mail addresses or other school systems. It is not acceptable to contact pupils using personal equipment or personal contact details, including your own mobile phone or through your personal social network profiles.
- Any online activity, including messages sent and posts made on websites, and including activity outside of school, should not bring your professional role or the name of the school into disrepute.
- Any still or video images of pupils and staff should be for professional purposes only. They should be taken on school equipment, and stored and used onsite. Such images should not be taken off-site without permission and valid reason.
- You will not give out your personal details, or the personal details of other users, to pupils or parents or on the Internet. In particular you should ensure your home address, personal telephone numbers and email accounts are not shared with children, young people or parents.
- You should ensure that any personal or sensitive information you use or access (e.g. SIMS data, assessment data) is kept secure and used appropriately.
- Personal or sensitive information should only be taken off-site if agreed with the Headteacher, and steps should be taken to ensure such data is secure.
- You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.
- You should support and promote the school E-Safety Policy, and promote and model safe and responsible behaviour in pupils when using ICT to support learning and teaching

You understand that your files, communications and Internet activity may be monitored and checked at all times to protect your own and others' safety, and action may be taken if deemed necessary to safeguard yourself or others. If you do not follow all statements in this AUP and in other school policies you may be subject to disciplinary action in line with the school's established disciplinary procedures.



### Appendix 3

# Burlington Junior School

## Use of Google Classroom/Google Meet

Please read the following expectations in regards to your child's attitude and behaviour for home learning. This MUST be completed and signed by a parent or carer before they can join any live sessions/activities with a member of teaching staff.

1. Pupils will never use email or other communication tools to offend, intimidate, exclude or in any way 'bully' others.
2. When working collaboratively, pupils must ensure they do not interfere with, delete or alter others' work unless they are offering constructive feedback. This includes deliberately deleting, amending or editing others' saved work without their, or their teacher's, explicit permission.
3. Pupils must not change any setting on their Chromebook without permission from their class teacher or other designated member of staff.
4. Pupils must report any problem, concern or incidents which they feel uncomfortable about, to their class teacher or other member of staff and refrain from sharing personal information about themselves whilst online, as detailed in the school's e-safety input.
5. Pupils must ensure they only ever use appropriate images, videos, text and other media in all their work and use of this technology.
6. Pupils must ensure that the camera on the device is not used to record anybody without their permission.
7. When using 'Google Meet' you must be dressed appropriately and join all meetings on mute.
8. When pupils are completing their lessons, they must ensure they are in a room where they can concentrate without distractions.
9. When pupils are using 'Google Meet' they must be aware of any background noise that will come through their microphone when speaking.

We want every child at school to enjoy and have a positive experience using the latest technologies to enhance their remote learning. Following the above rules and guidance will help us to achieve these goals.

Pupil name:

Signed (parent):

Signed (child)