E-Safety Policy

Acceptable Use Policy for Belvue School

2020/21

Contents

Introduction

Computing in the 21st Century is seen as 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, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of Computing within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting (Audio Sharing)
- Video Sharing
- Music Sharing / Downloading
- Gaming
- Mobile / Smart phones with functionality including: text, video, web, audio, music , global positioning (GPS)
- Other mobile devices with similar functionality (tablets, laptops, gaming devices)

Whilst exciting and beneficial both in and out of the context of education, much Computing, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

Ensuring children and young people are aware of the risks associated with the use of technologies, and can adopt safer behaviours, is vital in safeguarding them against cyber-bullying and grooming.

At Belvue School we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

This policy relates to both fixed and mobile Internet technologies provided by the school, and technologies owned by pupils, parents and staff, but brought onto school premises.

Roles and Responsibilities

The Head and governors have ultimate responsibility to ensure that this policy and its practices become embedded and are monitored. The named e-Safety co-ordinator in our school is Dawn Carmicheal-John who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the co-ordinator to keep abreast of current issues and guidance through organisations such as Ealing LA, CEOP (Child Exploitation and Online Protection), UKCCIS, and Childnet.

Senior Management and Governors are updated by the Head / co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour / pupil discipline (including the anti-bullying) policy and particularly to the curricular for PHSE and RSE.

Skills / awareness development for staff

- Our staff receive regular information and training on E-Safety issues in the form of staff briefings and CPD
- Details of the ongoing staff training programme can be found on the teacher drive, training.
- New staff will receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- All staff are expected to incorporate activities and awareness within the Computing, PSHE and SRE curriculum areas.

Managing the school e-Safety messages

- We endeavour to embed messages across the curriculum whenever the Internet and / or related technologies are used. This is particularly reinforced in PSHE, Vertical tutor time and RSE lessons in relation to cyber-bullying and to grooming.
- The policy will be introduced to the pupils at the start of each school year.
- Posters will be prominently displayed in each classroom and in the Computing suite.
- The school uses Sophos and LgFL filtering software.

Computing in the Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for guidance to be given to the pupils on a regular and meaningful basis. This is embedded within our curriculum and we continually look for new opportunities to promote.

- The school has a framework for teaching in Computing / PHSE / RSE lessons
- The school provides opportunities within a range of curriculum areas to support his or her learning effectively and creatively. To support the use of a range of Computing tools in a relevant curriculum context, this will enable students to build and develop their confidence in his or her use of Computing, making the learning experience enjoyable.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are aware of the relevant legislation when using the Internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know 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; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.
- PSHE, SEAL & RSE lessons provide the opportunity to discuss issues relating to cyber-bullying and Internet grooming (e.g. through respect for others and appropriate / positive relationships) These lessons can equip pupils with the knowledge to keep safe from harm.
- The school refers to the PSHE & RSE schemes of work in the PSHE section of the Local Authorities "Healthy Schools room" on the MLE (Managed Learning Environment).

:

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, not even with their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read ***and sign*** an Acceptable Use Agreement to demonstrate that they have understood the school's Policy.
- Users are provided with an individual network, email and Learning log-in username. From Year 7 they are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If a user thinks their password may have been compromised or someone else has become aware of their password they are expected to report this to their Vertical Tutor or class teacher.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMs systems and including ensuring that passwords are "strong", not shared and are changed periodically. Individual staff users must also make sure that workstations are not left logged on, but instead are locked. The automatic log-off time for the school network is 5 minutes.

- In our school, all Computing password policies are the responsibility of Jennifer Vaughan and all staff and pupils are expected to comply with the policies at all times.

- Staff will use "strong" passwords for all school related accounts:
  e.g.1cw2g2F = I can't wait to go to France

:

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- The school network is backed up daily using tapes. These tapes are stored securely off site by the Premises Manager.
- Google Workspace the remote learning platform complies with the GDPR G Suite Data Protection Implementation Guide

- **Staff will:**
- Ensure any paper files held at home are in a locked cabinet.

- Never save any personal information to their own computer / device. Only save to encrypted, password protected /school issued devices.
- Access school network resources / computers remotely using LGfL Remote Access (RAv3) as specified by the head teacher and set up by the technician. School Leaders can access Sims/teacher drive/Leadership drive. The school data manager has remote access to SIMs.

- Not allow family members or friends to use the computer while logged in remotely to school resources.

- Not leave the leave the computer/iPad unattended while logged in remotely to school resources.

- Never share passwords / leave on post-it notes etc.

:

Managing the Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. In our school access to the Internet is via the London Grid for Learning. Internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- In our school students have supervised access to the internet
- Some students in year Post 16 and Year 11 have unsupervised access to Internet resources through the school's fixed and mobile Internet technology.
- Staff will preview any recommended sites before use with students.
- Raw image searches (e.g. Google image search) are discouraged when working with pupils. The LGfL photo gallery is used in class **www.gallery.lgfl.net**
- If Internet research is set for homework, specific sites will be suggested. These will have been checked by the teacher. Where possible links from the school learning platform will be provided,
- It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastucture

- The London Grid for Learning (LGfL) provides, upon request, the facility to monitor and log web-based activity.
- School Internet access is controlled through the LGfL's web filtering service (WebScreen2).
- In addition, our school also manages some bespoke web filtering which is the responsibility of Trusol.
- Belvue School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.

.

Managing the Internet

- The school does not allow pupils access to Internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the co-ordinator. / They are encouraged to click on the Hector Dolphin screen image. The offending URL will be reported to LGfL and / or the school technician Turniton.
- Sophos Anti-Virus protection is provided by the LGfL and is set to automatically update on all school machines. This is the responsibility of our network support team from Turniton.
- In addition any staff laptops used at home should also be protected by Sophos Anti-Virus (as under the LGfL licence)
- Pupils and staff are not permitted to download programs or files on school equipment without seeking prior permission from the Headteacher
- If there are any issues related to viruses or anti-virus software, Turniton technician should be informed in person or a message left in his communication book.

Managing other Communication & Networking technologies

: The Internet includes a wide range of communication and networking tools & sites. Children need to be educated about appropriate ways of communicating and about the risks of making personal information too easily available. If used responsibly outside and within an educational context it can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school denies access to social networking sites to pupils within school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images/videos of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are asked to report any incidents of bullying to the school.
- Pupils are introduced to a variety of Internet communication tools within the safe context of the school learning platform / London MLE/Google Workspace.
- Staff understand that it is highly inappropriate to use social networking sites and other personal communication tools to communicate with pupils and / or parents (e.g. Facebook, Twitter, Instagram, Snap Chat, email, MySpace etc.).
- Staff understand that it may considered a disciplinary offence if they mention on social networking sites; issues concerning students / parents / carers / other staff associated with the school.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies (such as portable media players, gaming devices, smart phones, etc.) are familiar to children outside of school. Allowing such personal devices to access the school network can provide immense benefits in collaboration, but also create risks associated with misuse, inappropriate communications, etc. Emerging technologies will be examined for educational benefit and the risk assessed before such use of personal devices is facilitated in school. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device on school premises.
- When working remotely staff can use their personal mobile phones to contact pupil/parent but must ensure their number is protected by using 141 before entering pupil or parents number.
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched to silent mode. Is this still practiced?
- Technology may be used, for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages and photos between any member of the school community is not allowed.
- Permission must be sought before any image, video or sound recordings are made on these devices of any member of the school community.
- Capturing images & video is not allowed by students / staff unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages and photos between any member of the school community is not allowed.
- Permission must be sought before any image, video or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies (e.g. phones, laptops, etc) for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop and iPad for staff, only this device may be used to conduct business outside of school.

Managing Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and be aware of what constitutes good 'netiquette'. In order to achieve Computing level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all staff an individual account to use for all school business via LGfL. This is to minimise the risk of receiving unsolicited or malicious emails and that of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. Staff outlook exchange mail should used for all school business.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder. This is currently being set up automatically.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staffs sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated office account.
- Pupils may only use school approved emails (LGfL LondonMail and the school Google Workspace account on the school system and only under direct supervision for education purposes. When learning remotely students will use this learning platform under direct supervision of their parents/guardians.
- Outlook exchange is subject to mail scanning.
- The forwarding of chain letters is not permitted in school.
- All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive message and keep the offending message(s) as evidence.
- Staff must inform (the co-ordinator/ line manager) if they receive an offensive email.
- Pupils are introduced to email as part of the Computing Scheme of Work in Year 7.

Safe Use of Images / Video

Taking of Images and Video

Digital images / video are easy to capture, reproduce and publish and, therefore, easily misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images / video by staff and pupils with school equipment.
- Staff are not permitted to use personal devices, (e.g. mobile phones and cameras), to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal devices, (e.g. mobile phones and cameras), to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.

Consent of adults who work at the school

- Permission to use images / video of all staff who work at the school is sought on a regular basis and a copy is located in the personnel file
- Parents/Guardians must seek permission to take photos / video school events, and must agree to NOT post images / video on the Internet.
- Parents/Guardians are requested NOT to video school performances. Video are captured ONLY by school staff and are stored on the school secure service system and made available on the school website.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos/ video in the following ways:

- On the school website
- In the school prospectus and other printed publications that the school may produce for promotional purposes
- Recorded/ transmitted on a video or webcam
- 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).

Safe Use of Images / Video

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/Guardians may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

- Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.
- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.
- Only the Web Manager has authority to upload to the public website.

Storage of Images / Video

- Images/ video of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media (e.g. USB storage devices) for storage of images without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network video of pupils are deleted when pupils leave the school.
- Jennifer Vaughan has the responsibility managing the deletion of the images when specified.

Webcams and CCTV

- We do not use publicly accessible webcams in school other than for special projects such as nature cams which are streamed to the web.
- Webcams in school are only ever used for specific learning purposes, (e.g. monitoring hens' eggs) Images of children / adults ever never broadcast.
- Webcams is only used for staff training / development with the agreement / permission of the staff concerned
- Misuse of a webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
- Webcams are stored with the humanities resources for educational purposes.

Safe Use of Images / Video

Video Conferencing:

We have introduced the Google Workspace platform to allow students to continue learning remotely.

- Permission would be sought from parents and carers if their children were involved in video conferences.
- Permission would be sought from parents and carers if their children were involved in video conferences with end-points outside of the school.
- All pupils would be supervised by a member of staff when video conferencing
- All pupils would be supervised by a member of staff when video conferencing with end-points beyond the school.
- The school would keep a record of instances of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- No part of any video conference would be recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Misuse and Infringements

Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher. Incidents should be logged (see Incident Log in Appendix) and process should be followed (see Flowchart in Appendix).

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the co-ordinator, and depending on the seriousness of the offence may lead to:
    - Reporting to the Child Protection / Safeguarding Officer via My Concern
    - Investigation by the Headteacher / LA
    - Immediate suspension
    - Dismissal
    - Involvement of police

- Users are made aware of sanctions relating to the misuse or misconduct by the e-safety and data protection agreement they sign.

Pupils with additional needs

The school endeavours work in partnership with parents to convey a consistent message to all pupils. This in turn should aid the establishment and future development of the schools' rules.

Staff are aware that some pupils will require additional reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Activities are planned to make use of best available resources and are carefully managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school while appreciating the benefits provided by technologies generally. We regularly consult and discuss with parents/ carers and seek to promote a wide understanding about the link between technology and safeguarding.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school policy by consultation through the web-site.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation

- Staff and pupils have been involved in making/ reviewing the policy through circulation to all staff and staff discussion of the policy.

Review Procedure

There will be an on-going opportunity for staff to discuss with the coordinator any issue of e-Safety that concerns them.
This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.
The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.
This policy has been read, amended and approved by the staff, head teacher and governors in June 2020.

Acceptable Use Agreement: Staff, Governors and Visitors

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

The school Acceptable Use Policy is designed to ensure that all staff are aware of their responsibilities when using any form of Information & Communications Technology within their professional role. All staff are expected to sign this policy and adhere at all times to its contents.

- I will comply with the Computing system security protocols and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role, and never via personal email / phone accounts / social networking profiles.
- I will not discuss school issues on social networking sites / web-blogs.
- I will not give out to pupils, my own personal contact details, such as mobile phone number and personal email address.
- I will only use the approved, secure email system(s) and MLE tools for communications related to my professional role.
- I am aware that communicating with students / pupils via private email / SMS and social networking sites may be considered a disciplinary matter.
- 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.
- I will ensure that I only take school personal data off school site in encrypted form, or will access the data remotely.
- I will not install any hardware or software without permission of the Computing leader.
- I will not browse, download, upload or distribute any material of a pornographic, offensive, illegal or discriminatory nature. **I understand that to do so may be considered a disciplinary matter, and in some cases a criminal offence.**
- Images & videos of pupils and / or staff will only be taken, stored on school equipment and will only be used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images & video will not be distributed outside the school network / MLE without the permission of the parent/ carer, member of staff or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of Computing and related technologies.

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

Signature ……..…….…… …….Date ……..

Full Name …….....(printed)

Job title……

Acceptable Use Agreement: Pupils - MLD

Pupils Acceptable Use

Agreement / e-Safety Rules

- ✓ I will only use Computing in school for school purposes.
- ✓ I will only use my class email address or my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my passwords or use anyone else's.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all Computing contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using Computing because I know that these rules are to keep me safe.
- ✓ I know that my use of Computing can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.
- ✓ I will not give private details (home address, mobile number, email address etc.) to people I meet online.

Acceptable Use Agreement: Pupils - MLD

Secondary Pupil Acceptable Use Agreement / e-Safety Rules

- ✓ I will only use Computing systems in school, including the Internet, email, digital video, mobile technologies, etc. for school purposes.
- ✓ I will not download or install software on school technologies.
- ✓ I will only log on to the school network/ Learning Platform with my own user name and password.
- ✓ I will follow the schools Computing security system and not reveal my passwords to anyone and change them regularly.
- ✓ I will not use anyone else's username and password.
- ✓ I will only use my school email address.
- ✓ I will make sure that all Computing communications with pupils, teachers or others is responsible and sensible.
- ✓ I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- ✓ I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- ✓ I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- ✓ Images of pupils and/ or staff will only be taken, stored and used for school purposes inline with school policy and not be distributed outside the school network without the permission of Belvue School.
- ✓ I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- ✓ I will respect the privacy and ownership of others' work on-line at all times.
- ✓ I will not attempt to bypass the Internet filtering system.
- ✓ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- ✓ I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Belvue School
Rowdell Road
Northolt
Middlesex
UB5 6AG

Tel: 020-8845-5766

e-mail : head@belvue.ealing.sch.uk

Dear Parent/ Guardian

Computing including the Internet, email and mobile technologies etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any Computing.

Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact your child's vertical tutor.

_____✂_____

Return Slip: **Acceptable Use Agreement and E-Safety Rules: Pupils**

Parent/ Guardian signature

We have discussed this and …….....(child name)

Agrees to follow the e-Safety rules and support the safe use of Computing at Belvue School.

Parent/ Guardian Signature ……..……..……..

Tutor Group: ……. Date: …….