Believe - Learn - Succeed

Beaudesert Lower School

E Safety Policy 2023/2024

Date of Policy	September 2023
Review Date	September 2025

E-SAFETY

Rationale
The school encourages use by pupils of the rich information and interactive resources available on the internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills are fundamental in the society to which our pupils belong.

On-line services open classrooms to a broad array of resources. In the past, teaching and library materials could usually be carefully chosen. All such materials would be chosen to be consistent with national policies, supporting and enriching the curriculum while taking into account the varied teaching needs, learning styles, abilities and developmental levels of the pupils. Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by teachers as appropriate for use by pupils.

Electronic information research skills are fundamental to the preparation of citizens and future employees. The school expects that staff will investigate possibilities and blend use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the appropriate use of such resources. Staff will consult the Computing coordinator for advice on content, training and appropriate teaching levels. Any content to be used as part of the Creative Curriculum must also be considered.

Access to on-line resources will enable pupils to explore thousands of libraries, databases, and activities. The school believes that the benefits to pupils from access to information resources and increased opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to allow pupils internet access within the school environment.

School Procedures
Resource Development
In order to match electronic resources as closely as possible to the national and school curriculum, teachers need to review and evaluate resources in order to offer materials that are appropriate to the age range and ability of the group being taught. The class teacher will provide appropriate guidance to pupils as they make use of the internet to conduct research and other studies. All pupils will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

While pupils may be able to move beyond those resources which have been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Pupils may not pursue electronic research independent of staff supervision. The school's internet access is controlled by filtering software chosen by London Grid for Learning, which should stop access to many inappropriate sites, although we recognize that no system is totally secure.

The staff are aware that all inappropriate sites accidentally accessed in school should be reported to the Computing Coordinator, Headteacher and then to London Grid for Learning. It must also be logged on the school incident record sheet which is available in the Computing Co-ordiator File.

Acceptable Use Policy

The requirement to ensure that pupils, staff and, indeed, all others in the school community are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound. This framework of e-safety, or acceptable use policy (AUP), is to promote safe and appropriate use. As such, it should be understood in the context of other 'child protection' and 'behavior' policies that the school already has in place as well as other existing policies in respect of its employees.

Given the glittering array of new technologies now available to use for educational purposes and in everyday life, the intention of this evolving policy is:

- To maximize e-safety for all members of the school community
- To help everyone understand the potential risks
- To provide guidelines (including how the policy will be regulated and any sanctions) for safe and appropriate school and home use as such, the school more specifically intends:

- To provide a secure network for the school and secure means of home/school access
- To monitor traffic, log incidents and act accordingly
- To establish key standards and behavior for e-safety across the school, in keeping with those of the Local Authority
- To co-ordinate the activities for the school related to promoting best practice in e-safety, including the publication of guidelines and acceptable use policies for pupils, staff, parents and governors
- To ensure that we adhere to e-safety issues related to new government policies affecting schools
- To monitor the school's responses to e-safety matters and act accordingly
- To have a named Senior Information Risk Officer – (SIRO)(Headteacher) – to co-ordinate the development and implementation of e-safety policies, with clear designated responsibilities, and liaise with the Local Authority in such matters

E-safety is a whole-school issue, not something that is simply the responsibility of the Computing coordinator. As such, the whole school has a responsibility to promote it.

Guidelines for AUP

The AUP aims to:

- Reflect the understanding that all members of the school community have responsibilities towards themselves, towards others and towards the school and that these responsibilities are not confined to the physical location of the school.
- Enable young people to develop their own protection strategies when adult supervision and technological protection are not available
- Provide information on where to seek help and how to report incidents (CEOP – www.thinkuknow.co.uk)
- Help young people understand that they are not accountable for the actions that others may force upon them, but that there are sanctions that the school will impose if they act inappropriately when online
- Provide guidelines for parents, carers and others on safe practice
- Ensure that the practice that it promotes is regularly monitored and reviewed with stakeholders
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

Strategy

This policy is the result of ideas discussed by the school community. The policy has been put to the school staff and ratified by the Governors. Parents are informed through the home/school agreement, guidelines distributed during Parents' Evenings and the pupils' AUP which is signed by them and their children at the beginning of the school year. E-Safety guidelines are displayed in the computer areas.

Passwords

Staff and pupil passwords are kept private and only the holder can change them. It is accepted that from time to time, e.g. forgetting a password, the ICT technician/School Business Manager can help to create a new password but s/he will not know what it is. Computers must not be left in 'logged on' mode. It is good practice for users to change their **passwords regularly.**

Access to all Computing systems shall be via logins and passwords. Any exception must be SIRO approved. All information storage shall be restricted to necessary users with any additional access being SIRO approved. The SIRO must maintain a record of who has access to restricted information.

Restricted **(Named staff only)**	**Protected** **(All in school community)**	**Public** **(Anyone)**
Any information that identifies an individual	Routines, management information	Website, parent mail, display

Emails

It is accepted that staff may send emails using their school Gmail account and attachments to recipients outside the school. Children may only do so under the supervision and direction of their teacher.

Anti-virus and anti-spam system

The school has an up to date anti-virus and anti-spam system provided by the London Grid for Learning which is updated weekly. The network is set up to automatically scan laptops and other portable devices every time they are connected to the school system.

Inappropriate content and language

There will be zero tolerance to the use of inappropriate content and language on any Computing equipment within our school community.

The type of language that is used in emails should be no different to that which is used in face to face situations.

Inappropriate Web content:

1. Chat rooms/instant messaging (except that promoted by the school for educational purposes)
2. Newsgroups/forums (except that promoted by the school for educational purposes
3. Internet peer to peer networks
4. Downloads of ring tones, screensavers and games (except any promoted by the school for educational purposes)
5. Downloads of freeware, shareware, evaluation packages (except by authorized persons and in compliance with copyright law)

The SIRO will maintain an incident log and report on its use once a year to the governing body. One log (as seen below) will be kept in each computer area.

Beaudesert Lower School

E-safety Incident Record

Date of incident	Time of Incident	Computer Used	Person Involved	Person Dealing with the incident	Evidence	Who was Consulted	Measures Taken	Who was Informed

Staff

The school aims to establish a clear understanding of the responsibilities of all those involved in the education of children and young people with regard to e-safety during staff training sessions. It is expected that all staff will read (and if necessary seek clarification) all school policies. Working at this school means acceptance of those policies including this AUP.

As such:

- Staff must not allow any emails between themselves and pupils to be anything other than school business.
- Staff must not have any pupil (or former pupils) as 'on line' friends if they are of school age. Staff must report to the SIRO any contact from a pupil or former pupil of school age.
- During Computing lessons pupils should be made aware of the procedures for reporting accidental access to inappropriate materials. In any instance of deliberate misuse, the SIRO must be informed and the pupil will be dealt with in accordance with the school's behavior policy.
- The school email accounts may be used for staff's personal use.
- Staff need to be aware that conducting any personal transactions could result in residual information remaining on the hard drive which may be accessible to others. **Neither the school nor the Local Authority can accept any liability for any resulting loss or damage.**
- Staff should keep to a minimum any data which is held on their school laptop and they must lock it if it is left unattended (ctrl + alt + delete, lock). The security of school laptops out of school lies with the staff who, by taking them off school premises, accept responsibility for them.
- PCs and laptops for pupils must be arranged in classrooms to allow good teacher supervision. Whole class teaching of Computing must be supported by an additional member of staff.
- It is not appropriate for staff members to use personal camera phones to photograph the pupils. Images taken on digital cameras (whether personal or school property) must be transferred onto the school system under the direction of the ICT technician and not removed from school premises.
- All photographs containing children must be stored on the school network by the teachers who will arrange for the deletion of them within two years of the child leaving unless parental permission has been given to retain them longer e.g. for publicity purposes).
- The use of memory sticks or external hard drives is not recommended and all data should be saved on the staff drive or shared drives. Should they be permitted by the headteacher, it MUST be security encrypted and comply with GDPR regulations.

Pupils

Pupils are involved, through the School Council and the work done in Computing lessons or computing club in which activities to promote good practice and internet safety issues are delivered, in the evolution of this AUP and the following guidance:

- Pupils are not encouraged to bring in to school personally owned devices unless they have been so requested by their teacher. Any such device should be handed into the school office for safekeeping until such time as they are required or collected at the end of the school day.
- The school cannot accept any responsibility for personally owned devices (e.g. laptops, mobile phones and digital cameras) brought into school or taken on educational visits. If these are to be used on the school network they must, on a daily basis, first be virus checked by the ICT Technician before they are connected or used. They can only be taken on educational visits at the discretion of the teacher in charge and provided that pupils agree to use them appropriately as they would in school.
- School data should not be stored on these devices other than for the time it is actually being used.

- The school accepts the use of school email addresses by pupils in other schools providing they adhere to the pupil AUP.
- Pupils learn about the good practice that is appropriate for social networking through the use of the thinkquest.org which they are introduced to during Computing lessons in Key Stage 2.
- Pupils are made aware of the procedures for reporting accidental access to inappropriate materials before using the internet.

If children accidentally find inappropriate material they are to report it to their teacher who will alert the SIRO so that s/he can take steps to rectify this. Staff who find inappropriate material will report it directly to the SIRO. Children learn of this procedure in their lessons and it is reinforced. Staff are made aware of their responsibilities in this during staff training and by having their own copy of the policy.

Sanctions
Pupils who deliberately abuse the AUP will be dealt with in line with the school's Behaviour Policy. Parents must be informed and any incident must be logged in school by the SIRO,

This policy will be reviewed within one year of its first ratification by the school Governors

Pupil Guidelines for Internet Use

General
Pupils are responsible for good behavior on the internet just as they are in a classroom or a school corridor. General rules apply.
The internet is provided for pupils to conduct staff guided research and communicate with others. Remember that access is a privilege, not a right and that access requires responsibility.
Individual users of the Internet are responsible for their behavior and communications over the network. It is presumed that users will comply with school standards and will honor the values the school holds. School may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks will always be private.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear responsibility for such guidance, as they must also exercise with information sources such as television, telephones, movies, radio, android devices, tablets, iPod, kindles, handheld consoles that link to the internet and other potentially offensive media.

The following will not be tolerated:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing or insulting others
- Damaging computers, computer systems or computer networks
- Violating copyright laws by downloading copyrighted items
- Using others' passwords
- Trespassing in others' folders, work or files

Sanctions
Violations of the above rules will result in a temporary or permanent ban on internet use in school.
Additional disciplinary action may be added in line with existing practice on inappropriate language or behavior.

Beaudesert Lower School

Keeping Safe with Computing

1. I will always ask the teacher before I use the Internet and will be sensible whenever I use it.

2. I will only use the internet for schoolwork or remote learning and will only use the sites my teacher has asked me to access.

3. I will not give my name, address, telephone number or photographs to anyone on the Internet and I will tell the teacher if anyone asks me for my name, address, telephone number or photograph.

4. I will talk to an adult if an online friend wants to meet me and never arrange to meet anyone without permission.

5. I will not download programs or bring a data storage device from home into school.

6. I will only email the people my teacher has approved and the messages I send will be polite and responsible.

7. I will report to an adult any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.

8. I realise that if I don't use the internet sensibly I will not be allowed to use it.

9. I will make sure that any passwords I know are kept secret and not shared with anyone.

10. I will make sure that I keep the Computing equipment safe and that I will not eat or drink whilst using it.