Online Safety Policy

Version Control

Version	Date	Author	Changes made:
0.1	1.9.17	Beth G	• Policy created
0.2	1.9.19	Beth G	• Updated
0.3	1.9.21	Anna B	• New logo added • Changed procedure for reporting online misuse • 'Learning platform' changed to the remote learning section of the school website
0.4	16.10.23	Lauren H	• Added a section to the Systems Security section: 'All Ipads and computers have filtering and safeguarding monitoring systems in place in line with KCSIE 23. Lauren Hirst (DSL) has access to check this and receive email notifications' • Added Ipads every time computers are mentioned. • 'Ensure that all Ipads and computers have filtering and safeguarding monitoring systems in place (in line with KCSIE 23), have access to check this and receive email notificationsF.' Added to safeguarding Leads responsibilities.

Online Safety Policy

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

This policy applies to all pupils, teaching staff, support staff, Governors and volunteers, as well as all other St Bede Primary Academy Extended Services.

Aims

Our aims are to ensure that *all* pupils:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid inappropriate material;
- will develop a positive attitude to the internet and develop their Computing capability through both independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

Internet use will support, extend and enhance learning

- pupils will be given clear objectives for internet use;
- web content will be subject to age-appropriate filters;
- internet use will be embedded in the curriculum.

Pupils' access to the internet

At St Bede Academy, we only allow children to use the internet when there is a responsible adult present to supervise.

All members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils the expectation we have of them.

Expectations of pupils using the internet:

- all pupils are expected to read (or be read) and sign the age-appropriate Children's Online Agreement;
- at St Bede, we expect all pupils to be responsible for their own behaviour on the internet, just as they are anywhere else in school. This includes materials they choose to access and language they use;
- pupils using the internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to switch off their screen and report it immediately to a member of staff, so that the service provider can block further access to the site;
- pupils are expected not to use inappropriate language in any online communications and contact only people they know or those the teacher has approved;
- pupils must ask permission before accessing the internet and have a clear idea why they are using it.
- pupils should not access other people's files unless permission has been given;
- computers should only be used for schoolwork and research unless permission has been granted otherwise;
- no program files may be downloaded to the computer/ Ipad from the internet. This is to prevent corruption of data and avoid viruses.

Pupils will use existing technologies safely

- pupils will be taught about how to stay safe online and what to do if they feel threatened, upset or vulnerable;
- they will be made aware of the risks when using the internet on digital devices, both in school and at home and will be encouraged to share their learning with parents/carers in the home environment.

E-mail

- pupils and staff will only use approved e-mail accounts when using the school network;
- pupils will tell a member of staff if they receive inappropriate e-mail communications;
- pupils will only use e-mail for approved activities.

Internet access and Purple Mash

- staff will read and sign the St Bede Primary Academy AIU Policy before using any school ICT resource;
- parents will give consent for their child to access the internet under supervision as part of their learning. This will be completed as part of yearly parental consent;
- pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult.

Systems security

- ICT systems security will be regularly monitored and reviewed by the schools ICT technical team and any problems reported to the senior management team. All Ipads and computers have filtering and safeguarding monitoring systems in place in line with KCSIE 23. Lauren Hirst (DSL) has access to check this and receive email notifications.

Communication of the Online Safety policy to pupils

- Pupils will read (or be read) and sign the age-appropriate Children's Online Agreement;
- Online Safety rules will be displayed in each room where a computer or Ipad is used;
- Pupils will be informed that internet and Purple Mash use will be monitored;
- Online Safety will be included in the curriculum and regularly revisited.

Communication of the Online policy to staff

- Acceptable Use Policy will be given to all new members of staff as part of the staff handbook;
- Staff will sign the Acceptable Use Policy and it will be kept in their staff HR file;
- The Online Safety and Acceptable Use Policies will be discussed with staff annually;
- Staff will be informed that internet and remote learning section of the school website use will be monitored.

Communication of the Online Safety policy to parents/carers

- The Online Safety policy will be available on the school website;
- The remote learning section of the school website will include Online Safety information for pupils and parents to access.
- The school will communicate Online Safety issues as necessary to parents through letters, the school website or on a one to one basis.
- The school will offer parental online safety training when necessary.

Online Safety complaints

- Staff will be trained so they are able to deal with Online Safety incidents.
- Instances of online misuse should be reported to the Designated Safeguarding Lead (L.Hirst)
- Reported incidents must be recorded on CPOMS.
- Pupils and parents will be informed of the consequences of online misuse.

Roles and Responsibilities.

Senior Management Team

- Support the Designated Safeguarding Lead and all staff in dealing with Online Safety issues as they arise.
- Dealing with any breaches of policy by staff members in line with the school Online Safety and Acceptable Use Policies.

Designated Safeguarding Lead

- Primary responsibility: establish and maintain a safe ICT learning environment.
- Ensure that Online Safety sessions are delivered to all pupils and revisited regularly.
- Respond to Online Safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies.
- Ensure that all staff have an awareness of Online Safety issues and are able to share these with the children as appropriate.
- Be responsible for maintaining professional development needs in this area.
- Ensure that all Ipads and computers have filtering and safeguarding monitoring systems in place (in line with KCSIE 23), have access to check this and receive email notifications.

Network Manager/Technical Support Staff

- Provide a technical infrastructure to support Online Safety practices.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.
- Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the DSL.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.

Teaching and Support Staff

- Contribute to the development of Online Safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of Online Safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Include Online Safety regularly in the curriculum.
- Deal with Online Safety issues they become aware of and know when and how to escalate incidents.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.

Wider School Community

- This group includes: non-teaching staff; volunteers; trainee teachers; other adults using school internet, the remote learning section of the school website or other technologies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of Online Safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.

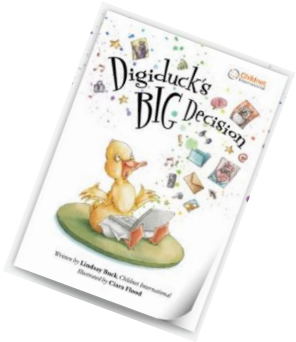
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.

Parents and Carers

- Read Online Safety policy and children's Online Safety agreement, encouraging their children to adhere to them.
- Give consent for their child to access the internet under supervision as part of their learning. This will be completed as part of yearly parental consent.
- Discuss Online Safety issues with their children, support the school in its Online Safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is involved with inappropriate behaviour online.

Key Stage 1 Rules for Online Safety

Remember...



'Think then Click'

I only use the internet when an adult is with me.

I will ask a teacher if I am not sure what to do or I think I have done something wrong.

I will look after the school's computing equipment.

I will only go on websites that my teacher has allowed.

I will tell my teacher if I go on a website by mistake.

I will always use what I have learned about online safety to keep myself safe.

I will tell a teacher if I see something that upsets me on screen.

At home I will tell a trusted adult if something upsets me online.

Key Stage 2 Rules for Online Safety

Remember...

'Think then Click'

I will only use the internet with an adult's permission.

I will tell an adult if I see anything I am uncomfortable with.

I will only use websites that a teacher has allowed.

I will ask a teacher if I am not sure what to do or I think I have done something wrong.

I will look after the school's computing equipment and tell a teacher if something is broken or not working.

When logging on using my own username and password, I will keep it safe and secret.

I will save only school work on the school computer/ Ipad and will check with my teacher before printing.

I will log off or shut down a computer/ Ipad when I have finished using it.

I will report anything inappropriate to a trusted adult or an online agency EG CEOP, Childnet etc.

I will not take or distribute images of anyone without their permission.

I will not share personal information online.

I will be polite and responsible when communicating online.

I understand that certain sites/games have age restrictions to keep me safe and if I access these I may be putting myself at risk.

CLICK CEOP
Internet Safety

Childnet International