Acceptable Use / Online Safety Policy

(IT) Policy

1 Introduction

1.1 Information Technology (IT) 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 arm our young people with the skills to access life-long learning and employment.

1.2 IT 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 IT 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
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much IT, 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.

1.3 At **Barnard Grove Primary School** we understand the responsibility to educate our pupils on Online 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.

1.4 Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile Internet technologies provided by the school (such as PCs, laptops, Chromebooks, webcams, whiteboards, digital video equipment, etc.)

1.5 Disclaimer**:** Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will, however, endeavour to add any important issues to the policy on our website.

2 Roles and Responsibilities

2.1 As Online Safety is an important aspect of strategic leadership within the school, the Headteacher and Local Academy Committee (LAC) have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

2.2 It is the role of the Online Safety Co-ordinator (Mr. Richard Whitham) to keep abreast of current issues and guidance through organisations such as Hartlepool LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

2.3 LAC Members are updated by the Headteacher/Online Safety Co-ordinator on any issues, and changing strategies at our school, in relation to local and national guidelines and advice.

2.4 This policy, supported by the school's acceptable use agreements for staff, LAC Members, visitors and pupils, is to protect the interests and safety of the whole school community.

3 Online Safety Skills Development for Staff

3.1 Staff receive regular information and training on Online Safety issues, in the form of staff meetings and notices; details of which can be found with the Online Safety Co-ordinator.

3.2 New staff receive information on the school's acceptable use policy as part of their induction.

3.3 All staff have been made aware of their individual responsibilities, relating to the safeguarding of children, within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart).

3.4 All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

4 Managing the school Online Safety messages

4.1 We endeavour to embed Online Safety messages across the curriculum, whenever the Internet and/or related technologies are used.

4.2 The Online Safety policy will be introduced to the pupils at the start of each school year.

5 Online Safety in the Curriculum

5.1 The school provides opportunities, within a range of curriculum areas, to teach about Online Safety. Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the Safety curriculum.

5.2 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.

5.3 Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.

5.4 Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. 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.

5.5 Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum in ***Year 3, 4, 5 & 6.***

6 Password Security

6.1 All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy.

6.2 Users are provided with a Learning Platform login username and password.

6.3 Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

6.4 If a password may have been compromised, this is reported to the Online Safety Co-ordinator.

6.5 Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and Learning Platform, including ensuring that passwords are not shared, and are changed periodically.

6.6 Due consideration should be given to security when logging into the Learning Platform to the browser/cache options (shared or private computer).

7 Data Security

7.1 The accessing of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. They must not:

- access data outside of school
- take copies of the data
- allow others to view the data
- edit the data, unless specifically requested to do so by the Headteacher and/or LAC.

8 Managing the Internet

8.1 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. OneIT filters, via Securly, all use of the Internet. Whenever any inappropriate use is detected it will be followed up.

8.2 The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile Internet technology.

8.3 Staff will preview any recommended sites before use.

8.4 Raw image searches are discouraged when working with pupils.

8.5 If Internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.

8.6 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.

9 Infrastructure

9.1 OneIT has a monitoring solution, via Securly, where web-based activity is monitored and recorded. School Internet access is controlled through One IT's web filtering service.

9.2 Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.

9.3 The school does not allow pupils access to Internet logs.

9.4 If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the teacher and then to the Online Safety Co-ordinator.

9.5 It is the responsibility of the school, by delegation to the service provider (OneIT) to ensure that Anti-virus protection is installed on all school machines.

9.6 Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus

protection software. It is not the school's responsibility, nor the service provider, to install or maintain virus protection on personal systems.

9.7 Pupils and staff are not permitted to download programs or files on school based technologies. If there are any issues related to viruses or anti-virus software, the Online Safety Co-ordinator/OneIT should be informed.

10 Mobile Technologies

10.1 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, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible Internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

10.2 Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately:

- The school allows staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a parent/ carer using their personal device. These devices should be kept out of sight of children at all times.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies, such as phones, laptops and PDAs, for offsite visits and trips, only these devices should be used.

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

11 Managing email

11.1 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.

11.2 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 good 'netiquette'.

11.3 The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

11.4 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. This should be the account that is used for all school business.

11.5 Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

11.6 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 trust'. The responsibility for adding this disclaimer lies with the account holder.

11.7 E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.

11.8 Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher and/or line manager.

11.9 Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.

11.10 All e-mail users are expected to adhere to the generally accepted rules of network etiquette, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus-checking attachments.

11.11 Pupils must immediately tell a teacher/trusted-adult if they receive an offensive e-mail. Staff must inform (the Online Safety Co-ordinator/ line manager) if they receive an offensive e-mail.

11.12 Pupils are introduced to email as part of the Computing Curriculum.

12 Safe Use of Images

12.1 Digital images are easy to capture, reproduce and publish and, therefore, 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.

12.2 With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

12.3 Staff are not permitted to use personal digital equipment, such as 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.

12.4 Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

12.5 On a child's entry to the school (and each year thereafter) all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Facebook Page
- 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, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the duration of the academic year 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/ carers may withdraw permission, in writing, at any time.

12.6 Images/ films of children are stored on the school computer.

12.7 Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher.

12.8 Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

12.9 We do not use publicly accessible webcams in school. Webcams in school are only ever used for specific learning purposes, i.e. animation and never using images of children or adults. Misuse of the webcam by any member of the school community will result in sanctions

12.10 Permission is sought from parents and carers if their children are involved in video conferences, including with end-points outside of the school.

12.11 All pupils are supervised by a member of staff when video conferencing and approval from the Headteacher is sought prior to all video conferences within school.

13 Misuse and Infringements

13.1 Complaints relating to Online Safety should be made to the Online Safety Co-ordinator or Headteacher. Incidents should be logged and the **Flowchart for Managing an Online Safety Incident** should be followed (see appendix).

13.2 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety Co-ordinator.

13.3 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart). Users are made aware of sanctions relating to the misuse or misconduct on the **Acceptable Use Agreement.**

14 Equal Opportunities

14.1 The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' Online Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

14.2 Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children.

15 Parental Involvement

15.1 Parents/carers and pupils are actively encouraged to contribute to the school Online Safety policy by letter and by reporting unsuitable sites etc to the Online Safety Co-ordinator.

15.2 Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school (and each year thereafter).

15.3 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).

15.4 The school disseminates information to parents relating to Online Safety where appropriate in the form of letters home or information on the school website.

16 Monitoring and Review

16.1 The monitoring of the standards of the children's work, and of the quality of teaching computing, is the responsibility of the subject leader (Mr. Richard Whitham). The computing subject leader is also responsible for supporting colleagues in their teaching of computing, for keeping informed about current developments in the subject, and for providing a strategic lead and direction for computing in the school. Areas of strength and weakness will be discussed with the IT team and SLT and priorities acted upon in order to improve further attainment and IT facilities.

Policy Reviewed: September 2023

Review Date: September 2024

Appendix:

Barnard Grove Primary Online Safety Incident Log

Details of ALL Online Safety incidents to be recorded by the Online Safety Co-ordinator. The Headteacher will monitor this incident log.

Date & Time	Name of pupil or staff	Male Or Female	Computer or Class	Details of incident (including evidence)	Actions and Reasons

Revised: September 2020

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / network, or other school systems.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: ...@banardgrove.adastraschools.org
- I will only use the approved Office 365 email system *and school approved communication systems* with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to OneIT and Kevin Stainsby.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other IT 'defence' systems*.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the school's guidance on use of mobile phones / devices at school and *will not take into classrooms / only use in staff areas*.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I will alert the school's child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to *senior member of staff* / *designated Child Protection lead*.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Head* / *Safeguarding Lead* on their request.
- *I will only use any trust system I have access to in accordance with their policies.*
- *Staff that have a teaching role only:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

User Signature

I agree to follow this code of conduct and to support the safe use of IT throughout the school.

Signature …… Date:.....…

Full Name ..... (printed)

Job title / Role .....

Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signature ..... ……Date.....

Full Name ..... (printed)

Flowchart for Managing an Online Safety Incident