Bladon C of E Primary School

Internet Use and Internet Safety (C18)

Date: November 2016 Review Date: November 2019

Authorised by: Approved by:

……..……. …….
(Tracey Fletcher, Headteacher) (Ray Banks, Chairman of Governors)

Purpose:
This policy will define the acceptable use of ICT (Information and Communications Technology) within our school and set out clear guidelines for all members of the school community.

The school community is defined as all those people (pupils, teaching staff, non- teaching staff, parents, visitors, governors, etc) who engage in learning, teaching, managerial and supportive activities within the confines of the school.

ICT resources are defined as:

- Any form of computing device (for example, servers, work-stations, lap-tops, tablet computers, calculators, ipads, mobiles) irrespective of any form of network connection;
- Any form of peripheral device(for example, a printer, scanner, digital still or video camera, control box, digital projector, microscope) that can be connected to any form of computing device or network connection and is capable of transmitting, receiving or responding to received data;
- Any form of computer or peripheral media, be it fixed or removable (for example, hard disc, USB, Memory Card, CD-ROM, floppy disc) that can transmit or receive data to or from any form of computing, peripheral or network device;
- Any form of software (for example, computer programmes such as word processors and image manipulators, or data files that record text, databases, sound, images, etc.) that is supplied on, or via, any form of media or transmission medium (for example, floppy disc, CD ROM or the internet).

User Responsibilities
The principles that are being applied are that members of the school community should:

- Behave at all times within the current legislation and the expectations of the school community;
- Only use school ICT resources to further curriculum, professional and managerial responsibilities or other uses that are sanctioned by the head teacher or governors;
- Make careful and considerate use of the schools ICT resources, report faults and work in a way that minimises the risk of introducing computer viruses to the system;
- Protect pupils in school from the harmful or inappropriate material accessible via the internet or transportable on computer media;
- No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.
- Users must not upload or download software on any device without the authorisation of the Headteacher.
- Users must take care to store sensitive information, e.g. pupil data safely and to keep it password protected, on all school systems, including laptops.

- No one may use ICT resources to transmit, download or upload any abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.
- No one may knowingly or willingly interfere with the security mechanisms or integrity of ICT resources. No one may use ICT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks.
- Staff are reminded that through their use of social media they must not post anything which would bring the school into disrepute.

School Responsibilities
The Governing Body is responsible for ensuring that employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.

If a member of school community has reason to believe that any ICT equipment has been misused and a member of the school community is in breach of this policy, they should consult the Headteacher. If the Headteacher believes that the matter needs external investigation (i.e. is a matter of Safeguarding) then they would contact the Local Authority Designated Officer (LADO). Alternatively they would contact HR for advice about disciplinary procedures. Internal school staff should not carry out any investigations either formal or informal unless authorised to do so.

Internet Access:
The Internet is an essential element in 21st Century life for education and is a key part of school curricula. It is, however, an open communications channel allowing information to be transmitted to many locations in the world with very little restriction. The purpose of this policy is to:

- Ensure that pupils benefit from all learning opportunities offered by the internet.
- Ensure internet resources provided by the school are kept safe and controlled.
- Ensure that all staff and pupils have clear guidance on safe and acceptable use.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the school's and personal items that are brought into school if applicable.

General:

- The ICT Coordinator and Head Teacher are responsible for the school's e-safety.
- Sophos virus protection software is used and updated on a regular basis.
- The school uses appropriate 'firewall' content filtering systems through our internet provider, ICT123 via businessband 6Mpbs with Exa Networks ADsl2+ broadband.
- The school works with ICT123 to ensure systems to protect pupils are subject to regular checks, to ensure that filtering methods are appropriate, effective and reasonable.
- ICT123 are contracted to provide on a fortnightly basis:
    - general website maintenance
    - resolution of all connection issues
    - upload apps/software as required
    - resolution of any wifi issues
    - advice on purchasing equipment
    - computer club support

1- INTERNET USE - Code of Practice:
The scope of this code covers fixed and mobile Internet; school PCs, laptops, i-pads and digital video equipment. Any devices owned personally by staff or pupils but brought onto school premises (such as mobile phones, camera phones, PDAs) are subject to the same requirements as technology provided by the school.

The ICT Co-ordinator will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Pupil access to the Internet is through a filtered service as described above. Parental permission is sought from parents before pupils access the Internet - see also Related School Documents Issued to Parents as listed on Page 3 and

available from the School Office. The measures outlined below are designed to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet.

- Children using the Internet will be working in the presence of the class teacher or other approved adult helper.
- Staff will check that sites pre-selected for children's use are appropriate for their age and maturity.
- Staff will be particularly vigilant when children are undertaking their own search and will ensure that they are following an agreed search plan.
- Children will be taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others.
- Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils acceptable use and risks.
- Teachers will have access to pupils' emails and other Internet related files, and will check these on a regular basis to ensure expectations of behaviour are being met.
- Methods to quantify and minimise the risk of children being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LEA, our Internet service provider and the DfES.

Pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable. Should an incident occur in which children are exposed to offensive or upsetting material, the school will respond to the situation quickly and on a number of levels:

- The class teacher and Head Teacher will give appropriate support to the children. The children's parents will be informed and given an explanation of the course of action taken.
- The ICT Coordinator will report the URL (address) and content of unsuitable sites to the Internet service provider and the LEA.
- All teaching staff will be made aware of the incident at the earliest opportunity

It is important for children to realize that they are expected to play their part in reducing the risk of viewing inappropriate material by obeying the rules of responsible Internet access. In particular:

- Pupils and staff consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources. They will also come under the general discipline procedures of the school.
- Pupils and staff using the Internet are expected not to deliberately seek out offensive materials. If any pupils or staff encounters any such material accidentally, they should report it immediately to the ICT Coordinator or Head Teacher in order that access to the site is blocked.
- Pupils are expected to contact only people they know or those the teacher has approved.
- They will be taught the rules of etiquette in email and are expected to follow them. Eg Pupils may only use the approved e-mail accounts on the school system.
- Pupils must ask permission before accessing the Internet and have a clear idea why they are using it.
- Pupils and staff should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses.
- No programs on disc or CD Rom should be brought in by pupils from home for use in school, although staff can seek permission from the Head. This is for both legal and security reasons.
- No personal information such as phone numbers and addresses should be given out.
- Uploading and downloading of non-approved software will not be permitted.
- There will be no access to social networking/gaming from school equipment.
- Pupils are advised that the use of social networking sites outside of school is inappropriate. This is reinforced with educational materials.
- Pupils must not share their usernames or passwords with anyone.

Internet access and home/school links:

- Parents will be informed in the school prospectus that children are provided with supervised Internet access as part of their lessons and will be kept informed of future developments by letter and newsletter.
- Parents and children will be expected to sign a permission form before they begin using the Internet to share responsibility with the school.
- Parents are required to inform the school if they have any objections to their child's work or photographs being published. If the parent has not specified a wish for their child to be excluded it will be assumed we have the parents' permission

School Website:

- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publication of children's work will be at the decision of the class teacher.
- The school website will avoid publishing the full names of individuals in a photograph.
- The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the web.

Related School Documents Issued to Parents:

- Code of Conduct for Use of the School's Internet/e-mail Facilities
- Data Protection Act
- Data we hold on pupils in school: Fair processing notice
- Internet Code of Conduct

2- MOBILE PHONE COMMUNICATION & INSTANT MESSAGING – Code of Practice

- No children are allowed mobile phones in school.
- If a child requires a mobile phone before or after school the child may take the phone to the office to be securely locked away until the end of the school day.
- Staff are not to give their home telephone number or their mobile phone number to pupils.
- Staff are not to make use of pupils' mobile phone numbers either to make or receive phone calls or text messages.
- Photographs and videos of pupils should not be taken with mobile phones.
- Staff should not enter into instant messaging communications with pupils.
- Staff should not take mobile phones into the classroom; they may be left in the staffroom. If staff expect to receive a call during lessons time they should direct the caller to the school landline in the office. If/when the call is made the member of staff will be informed by the office and, if essential, given time to leave the classroom to return or take the call.
- The school permits staff the use of personal mobile phones on school trips on the understanding they will never be used to capture still or video images.
- Staff are asked to ensure they are in possession of their mobile phone if they are engaged in lone working on the school premises – this is a safety measure.

3- USE OF SOCIAL MEDIA – Code of Practice

Bladon Primary School understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

Bladon Primary School defines social media as any online platform that offers real-time interaction between the user and other individuals or groups including –

- Blogs
- Online discussion forums
- Collaborative spaces such as Facebook

- Media sharing services such as YouTube
- Micro-blogging applications such as Twitter

Social Media Use – Staff

We do not currently have a social media account in the school's name but we recognise that this could bring some benefits and do not exclude ourselves from operating one in the future.

The Friends of Bladon School (FoBS) currently have a Facebook page which they use to promote events. This is monitored and is subject to closure if it leaves the school vulnerable to detriment.

- Staff must not access social media during lesson times unless it is related to the learning activity
- Staff may use social media during their break times but not in front of pupils.
- Members of staff must not 'friend' or otherwise contact pupils through social media.
- If pupils attempt to 'friend' members of staff through social media they should ignore requests.
- It is strongly recommended that staff do not 'friend' parents of the school. It is understood that, due to our village setting, friendships may exist outside of school and to ban such 'friends' is unrealistic and impractical. If parents are known to staff only through school contact then it is inappropriate for the relationship to be furthered through social media.
- Members of staff should avoid identifying themselves as an employee of the school on social media.
- Members of staff must consider carefully the content of anything they post online and refrain from anything which is damaging to the school or any of its staff or pupils
- Where teachers or members of staff use social media in a personal capacity, they should make it clear that their views are personal. Staff should not make comments about the school.
- Teachers or members of staff must not post any information which could identify a pupil, class or the school.
- Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.
- Members of staff should be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.
- Members of staff should regularly check their online presence for negative content via search engines.
- If inappropriate content is accessed online, an inappropriate website content report form should be completed and passed on to the headteacher.
- Attempts to bully, coerce or manipulate members of the school community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter.
- Staff members should use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

Social Media Use – Pupils and Parents/Carers

- Pupils should not access social media during lesson time as the school does not advocate the use of social media sites for children in the primary age range.
- Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.
- Pupils must not attempt to "friend" or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they will be reported to the headteacher.
- If members of staff attempt to "friend" or otherwise contact pupils or parents/carers through social media, they should be reported to the headteacher.
- Parents are politely asked not to attempt to 'friend' members of staff known to them only through the school and to respect that personal contacts who are members of staff will not engage in any messages about the school through this media.
- Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.
- Pupils and parents/carers must not post content online which is damaging to the school or any of its staff or pupils.

- Pupils at Bladon Primary School should not sign up to social media sites that have an age restriction above the pupil's age.
- Social media websites such as Twitter; Facebook; YouTube etc are currently blocked by the school network's firewalls. Attempts to circumvent the network's firewalls may result in a ban from using school computing equipment, other than during closed, supervised exercises during ICT lessons
- Inappropriate content which is accessed on the school computers should be reported to the headteacher so that the site can be blocked.
- The final decision on whether access should be granted to a site will be made by the headteacher.

Cyber Bullying

- Cyber bullying is taken seriously.
- Incidents of cyber bullying will be dealt with and reported along the same chain as the Anti-Bullying Policy.
- Staff members should never respond or retaliate to cyberbullying incidents. Incidents should instead be reported as inappropriate, and support sought from senior staff member.
- Evidence from any incident should be saved, including screen prints of messages or web pages, and the time and date of the incident.
- Where the perpetrator is a current pupil or colleague, most cases can be dealt with through the school's own disciplinary procedures. This may be via the LADO in the case of a member of staff.
- Where the perpetrator is an adult, in nearly all cases, a senior staff member should invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.
- If the perpetrator refuses to comply, it is up to the school to decide what to do next. This could include contacting the internet service provider in question through their reporting mechanisms, if the offensive content breaches their terms and conditions.
- If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school will consider contacting the police.
- As part of our on-going commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of computing and PforC