E - SAFETY POLICY

September 2015

Introduction

Safeguarding is a serious matter; at Birchwood Junior School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as E-Safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an E-Safety incident, whichever is sooner.

The primary purpose of this policy is two fold:

- To ensure the requirement to empower the whole community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Birchwood Junior School website; Staff and Students must sign the Acceptable Use Policy when they join the school community. Upon return of the signed permission slip and acceptance of the terms and conditions, students and staff will be permitted access to school technology including the Internet.

Roles & Responsibilities

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any E-Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure E-Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of E-Safety at the school (ICT Governor – Cliff Penning)

Reporting to the governing body, the Headteacher has overall responsibility for E-Safety within our school. The day-to-day management of this will be delegated to a member of staff, the E-Safety Officer as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated E-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All E-Safety incidents are dealt with promptly and appropriately.

The day-to-day duty of E-Safety Officer is devolved to the ICT curriculum Leader (Matthew Davies).

The E-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.

- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all E-Safety matters.
- Engage with parents and the school community on E-Safety matters at the school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the E-Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical E-Safety measures in the school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support (Avalon IT).
- Make him/herself aware of any reporting function with technical E-Safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any E-Safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the E-Safety officer and Headteacher.
- Passwords are applied correctly to all users regardless of age

All Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any E-Safety incident is reported to the E-Safety Officer (and an E-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the E-Safety Officer or the Headteacher to make a decision.

All students are to be made aware of the E-Safety agenda. The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters and annual E-Safety days the School will keep parents up to date with new and emerging E-Safety risks, and will involve parents in strategies to ensure that students are empowered.

It is not felt that an E-Safety committee is needed at Birchwood Junior School at this time. Responsible individuals are fully aware of their role and any incidents are dealt with on an individual basis. This will be reviewed annually.

Counter-Terrorism/Prevent Duty:

More information regarding the Prevent Duty policy can be found at the following website.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

The school & Avalon IT constantly monitor on-going internet activity in relation to counter terrorism. Emails, internet activity are monitored daily through staff supervision, anti-virus malware, sporadic checks by Avalon IT & e-safety mentoring. Staff will be informed about The Prevent Duty act and the designated safeguarding leader will attend the WRAP course (Workshop to Raise Awareness of Prevent).
As part of e-safety education, the children are taught how to keep themselves safe from 'Culture' behaviour. '*Culture' behaviour is defined as: Young people becoming caught up in a pack mentality and becoming involved in inappropriate anti-social behaviour.* As schools have a more important role to play in relation to prevention, staff at Birchwood Junior School have been made aware of resources to aid in educating the children about radicalisation. These can be found at the following website.
http://www.saferinternet.org.uk/

Technology
Birchwood Junior School uses a range of devices including PC's, laptops, Apple Macs and Ipads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:
Internet Filtering – we use internet filtering through the Lincolnshire School Network (Currently working through Avalon IT) that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, E-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.
Email Filtering – we use the Avalon IT that prevents any infected email to be sent from the school or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.
Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB key drives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made.
Passwords – all staff and students will be unable to access any device without a unique username and password.
Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as key drives are to be scanned for viruses before use.

Safe Use of Technology
Internet – Use of the Internet in the school is a privilege, not a right. Internet use will be granted: to staff upon signing the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.
Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Students are permitted to use the school email system, and as such will be given their own email address.
Photos and videos – Digital media such as photos and videos are covered in the school's Photographic Policy, and is re-iterated here for clarity. All parents must sign

a photo/video release when joining the school; non-return of the permission slip will not be assumed as acceptance.
Social Networking – there are many social networking services available; Birchwood Junior School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Birchwood Junior School. No other social media will be used by staff or children within the school community.

- Blogging – used by staff and students in the school.
- Twitter – used by the school as a broadcast service

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.
In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the does not have copyright permission to use that resource; it will be removed within one working day.
Incidents - Any E-Safety incident is to be brought to the immediate attention of the E-Safety Officer, or in his/her absence the Headteacher. The E-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum
It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Birchwood Junior School will have an annual programme of training which is suitable to the audience.
E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. This is ensured through the Annual E-Safety Day taking place in the Spring Term, where all lessons during the day revolve around promoting E-Safety. As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.
The E-Safety Officer is responsible for recommending a programme of training and awareness for the academic year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

This policy will be reviewed annually.

Headteacher: Tracey Bowman **Date:** 21/09/2015

Chair of Governors: Brian Main **Date:** 21/09/2015