THE BARCLAY SCHOOL

eSafety
Policy into practice

Governor committee:	Conditions for Success	March 2016
	Full governing body	By email circulation
Prepared by:	Andrew Noon	March 2016
Policy due for review:	Personal Development, Behaviour and Welfare	March 2017

The Stevenage Inspire Federation

eSafety at Barclay – Policy into practice

This document further explains how our approach to e-Safety, as described in our eSafety policy, works in practice. As such, it may be useful to read this document alongside our formal policy.

Principles

We are committed to developing *Barclay* as an *inviting, purposeful, successful learning community*, working together to improve learning and teaching and to raise achievement to enable all our students to meet, with confidence, future challenges. We recognise that 21st Century learners will increasingly learn alongside and with new technologies and we want them to be e-safe.

We wish to develp as a flexible e-learning environment where:-

- appropriate and cutting edge resources can be accessed whenever and wherever they needed, including from home
- learning is enhanced by a range of personalised opportunities using ICT both in and out of the classroom
- students are e-confident, prepared for the digital age in the workplace and further learning

Purpose

Our formal policy outlines our commitment to eSafety and legal obligations. Ofsted have identified the main areas of risk for schools communities as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape', the hacking of social media profiles) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Inspecting eSafety, OFSTED 2013)

Roles and Responsibilities

In order to address this increasingly important and rapidly changing issue, we have introduced the following leadership, consultation and accountability structure.

E-safety – Key Responsibilities

e-Safety Co-ordinator (Deputy Head or Assistant Head)

- Ensure that staff are aware of their responsibilities under the policy and are given appropriate training and support to enable them to fulfil their responsibilities.
- Ensure that issues with e-Safety, are addressed within the curriculum
- Lead the e-Safety Group.
- Ensure the school remains "up to date" with e-Safety issues and guidance through liaison with the local authority e-Safety Office and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)
- Ensure the Headteacher, School Leadership Team and Governors are updated as necessary, including being aware of local and national guidance on e-Safety and they are updated annually on policy developments
- Ensure that students have appropriate access to education and guidance on e-Safety issues, through the curriculum, assemblies and targeted events
- Ensure that training, information and guidance is available for staff, parents and governors
- Ensure that incidents involving aspects of e-safety are recorded and monitored.
- Ensure that the appropriate actions are taken to address e-Safety concerns.
- Ensure that information from monitoring is used to inform decisions about how best to protect members of our school community.
- Ensure that a range of stakeholders is consulted as part of the on-going development of our e-safety strategy (students, parents, staff and governors)

e Safety Group (to consist of at least: a member of the Leadership Team, Child Protection Lead, IT Manager, Link Governor)

- Oversee the establishment and maintenance of a safe and secure learning environment and curriculum at The Barclay School.
- Support the e-Safety coordinator in developing and reviewing policies and procedures to ensure that Barclay is a safe community.
- Provide support and advice for the E-safety co-ordinator.
- With the e-Safety Co-ordinator, review the information generated by the log or esafety incidents and identify actions (including seeking out further advice) to address emerging patterns.

ICT Team

- Ensure the school network is safe and secure for all groups – consistent application of protocols and management and development of software
- Advise the e-Safety Co-ordinator and e-Safety group on e-Safety issues/technology and, where necessary, to provide such guidance to the Governing Body/Leadership Team/
- Ensure that all data held on Students and staff held within school has appropriate access controls in place.

Designated child protection team

- To record and track incidents with an e-Safety aspect to them and report these to Governors and to the e-Safety group

Student e-Safety representative group

- To advise the e-Safety Co-ordinator and the e-Safety team on current themes and patterns of use amongst young people.
- To advise on the best way to communicate messages about e-Safety to young people.

Teachers

- Promote, model and support safe behaviours in classrooms and ensure that eSafety procedures are followed

All Staff

- To read, understand, adhere to and promote the schools policies and guidance
- To ensure any digital communications with Students are conducted on a professional level, using only platforms approved by the Headteacher (See specific references below)

eSafety Education and Curriculum

Student eSafety Curriculum

eSafety themes are explored in a range of subject areas. Much of the work is done in PSCHE curriculum, where there are targeted lessons in Year 7 and, more extensively, in Year 9.

The issues surrounding eSafety are also addressed alongside other themes, such as personal safety, bullying and friendships/social networking. We believe that many eSafety issues stem from the low self-esteem of students and our 'Healthy Minds' programme covers topics such as resilience, self-image, and media influences.

Each year group receives awareness-raising assemblies on a regular basis. These will also be informed by sources of expert advice and internal eSafety monitoring.

A webpage as part of the *Barclay* website provides links to frequently updated, trusted websites which provide information and guidance about eSafety.

Staff and Governor Training

All staff and governors will receive formal eSafety training at least every 2 years, as part of Basic Child Protection training. New recruits receive this training as part of their initial Child Protection training. Additional training will be provided in response to specific concerns.

Parent and Carer Awareness and Training

The Barclay eSafety webpage contains links to trusted websites which provide information on electronic communication for parents and carers. These sites also provide advice and guidance on how to support young people in using the internet and other communication safely.

Managing the ICT infrastructure

The School Network

The security of the School network is maintained by the ICT team, under the leadership of the school IT Manager. Their role is to:

- Ensure the health of the network through the employment of appropriate anti-virus software etc. and network setup, so that staff and students cannot download

executable files
- Ensure that the filtering methods are effective in practice and that access to any website considered inappropriate by staff is removed immediately
- Prevent student access to internet logs
- Use individual log-ins for students and all other users
- Ensure that all students (and their parent/carer) have read, understood and signed an Acceptable Usage Agreement. (A copy of this is kept on file, and this ensures that parents provide consent for students to use the Internet and other technologies)
- Ensure that all staff sign an Acceptable Usage Agreement. (A copy of which this kept on their personal file)
- Provide advice and information on reporting offensive materials, abuse/bullying etc. available for Students, staff and parents

Internet, Email and Social Networking

At *Barclay* we recognise that access to the internet is an invaluable learning tool and vital for effective communication. Risks are minimised by

- The supervision of students using the internet within school at all times, as far as is reasonable
- The use of filtering which blocks sites that fall into categories such as pornography, race hatred, gaming, other sites of an illegal nature
- Ensuring all users know and understand what the "rules of appropriate use" are and what sanctions result for misuse (through induction and teaching)
- Ensuring 'blocks' are applied to chat rooms, social networking sites, music downloads and shopping sites, except those used for specific educational purpose
- Establishing that email and internet use are not private and the school reserves the right to monitor all emails and internet usage involving the schools IT facilities/ services
- Allocating an email address through the school domain- enabling students to access the email from school and at home
- Discouraging the use of personal email addresses, staff are instructed to use the school domain for all professional purposes
- Ensuring staff do not communicate with, or have details of, students via their personal email or social networking site account
- Ensuring that staff do not have student contact details on their personal mobile phones; except for the specific duration of a school trip/visit
- Ensuring that, where staff use Social Networking sites to communicate with students, parents and/or the wider community, the use of these sites is agreed in advance with the Headteacher and strict protocols are followed

Please note: Details of policy on passwords, use of equipment and digital images and complaints procedures are contained in our formal policy.

Appendix A – Response flow chart for safety concerns