UNIVERSITY OF BIRMINGHAM SCHOOL

University of Birmingham School

E-Safety Policy

September 2018

UNIVERSITY OF BIRMINGHAM SCHOOL

University of Birmingham School
E-Safety Policy

Review Frequency	Every two years		**Review date**	June 2017
Governing Committee Responsible	Teaching and Learning	**Approved(date)** 19 June 2017	**Next Due**	June 2019
Governor Approval (date)	23 July 2015		**Website**	
Staff Responsible	M Roden		**Date Produced**	10 June 2015

At the University of Birmingham School we refer to **Pupils** (who are in Years 7-11 and aged 11-16) and **Students** (who are in Years 12/13 and aged 17-18)

1 Introduction

1.1 The use of ICT will:

a) Contribute to the delivery of outstanding quality teaching and learning
b) Enable effective tracking, target setting and the management of intervention strategies
c) Enable appropriate assessment
d) Support effective internal and external communication.

1.2 However, there are inherent dangers of using this powerful tool in a school environment.

1.3 It is therefore essential that schools create a safe ICT learning environment that includes three main elements:

a) An effective range of technological tools
b) Policies and procedure to describe and maintain the acceptable use of the schools ICT services and facilities with clear roles and responsibilities
c) A comprehensive e-Safety education programme for students, staff and parents.

1.4 The e-Safety Policy has been written in accordance with our vision for the University of Birmingham School and is supported by the following school policies:

a) Prevention of Bullying Policy;
b) Behaviour and Exclusions Policy;
c) Safeguarding Policy;
d) Complaints Policy, and;
e) Assessment, Recording, Reporting and Marking Policy.

2 Key Principles

2.1 All students should be able to learn in a safe environment and should not be exposed to inappropriate materials or cyber-bullying.

2.2 All staff are responsible for promoting and supporting safe behaviours in their classrooms and following the School's e-Safety Policy.

2.3 Students should feel and will be encouraged to be able to report any bullying, abuse or inappropriate materials for investigation.

3 Aims

3.1 To ensure students can learn in a safe and secure environment, in and out of school.

3.2 To minimise the risk of student exposure to inappropriate material or cyber-bullying.

3.3 To develop secure practice for students when communicating electronically.

3.4 To develop student self-responsibility when communicating electronically.

3.5 To ensure consistent good practice for staff when communicating electronically.

3.6 To ensure all staff are aware of issues relating to e-Safety.

3.7 To provide information, advice and guidance for parents/carers on the use of new technologies.

4 Roles and Responsibilities

4.1 Governing Body - ensure the e-Safety Policy is implemented, monitored and reviewed.

4.2 Senior Leadership Team:

a) Ensure, along with the Governing Body, that the e-Safety Policy is implemented, monitored and reviewed.

b) Ensure that all staff are aware of their responsibilities under the policy and are given appropriate training and support so that they can fulfil their responsibilities

c) Ensure that issues of e-Safety, including cyber-bullying, are addressed within the curriculum

4.3 Head of Computing:

a) Ensure the School remains 'up to date' with e-Safety issues and guidance through organisations such 'The Child Exploitation and Online Protection' (CEOP).

b) Ensure the Principal and Senior Leadership Team are updated as necessary, including being aware of local and national guidance on e-Safety and they are updated at least annually on policy developments

4.4 IT team:

a) Ensure the School Network is safe and secure for all groups – consistent application of protocols and management and development of software.

b) Advise Governing Body/Principal/Senior Leadership Team on e-Safety issues.

4.5 Teachers and Professional Services Staff - Responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures.

5 The security of the School Network:

This will be maintained by:

a) Ensuring its health through appropriate anti-virus software etc and network set-up so staff and pupil/students cannot download executable files (such as .exe .com .vbs etc).

b) Ensuring it is 'healthy' though robust monitoring on the network (this may be replaced or updated as appropriate to take account of technical and commercial developments).

c) Ensuring the IT Team is up-to-date with IT provider services for security.

d) Ensuring that the filtering methods are effective in practice and that access to any website considered inappropriate by staff is removed immediately (responsibility of the IT Team).

e) Not allowing students access to Internet logs.

f) Using individual log-ins for students and all other users.

g) Never sending personal data over the Internet unless it is encrypted or otherwise secured; or sent via secure systems such as the DfE s2s site.

h) Ensuring students only publish within appropriately secure learning environments such as their own closed secure log-in,

6 The Internet

6.1 The University of Birmingham School recognise that access to the internet is an invaluable learning tool and vital for effective communication.

6.2 Safety and security risks are minimised through:

a) The supervision of students using the Internet within school at all times, as far as is reasonable, and vigilance in learning resource areas where students have more flexible access;

b) The use internal filtering systems which block sites that fall into categories such as pornography, race hatred, gaming, other sites of an illegal nature;

c) Effective planning - internet use is matched to pupils' and students' digital competence;

d) Informing users that Internet use is monitored in the 'Acceptable Use of IT Agreement', and as part of our student induction process in ICT lessons;

e) Informing staff and students that that they must report any failure of the filtering systems directly to the IT Team or the classroom teacher;

f) Blocking all Chat rooms and social networking sites except those that are part of an educational network;

g) Only using approved 'blogging' or discussion sites;

h) Requiring pupils/students (and their parent/carer) to individually sign to say they will comply with the Acceptable Use of ICT Policy which is fully and used as part of the teaching programme. A copy is kept on file, and this ensures parents provide consent for students to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school.

i) Requiring all staff to be made aware of the Acceptable Use policy and that on signing their terms and conditions of employment they agree to comply with its contents;

j) Ensuring all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through induction and teaching programme;

k) Maintaining a record of any cyber-bullying or inappropriate behaviour and act to deal with the perpetrators of this behaviour;

l) Making information on reporting offensive materials, abuse and bullying etc available for students, staff and parents;

m) Immediately referring any material suspected of being illegal to the Police;

n) Establishing that e-mail and Internet use is not private and the schools reserve the right to monitor all e-mails and Internet usage involving the School's IT facilities and/or services;

o) Allocating an e-mail account through the school domain – enabling them to access their e-mail from school and at home through web connect system;

p) Ensuring staff do not communicate with students via their personal hotmail, MSN accounts or through their personal social networking site account (e.g. Facebook, Twitter etc.);

q) Ensuring staff only communicate with students via their designated School e-mail account;

r) Ensuring staff do not attempt to use their personal social networking site(s) in school;
s) Ensuring staff do not communicate with, or have details of, students on their personal social networking account or any other electronic device e.g. Facebook;
t) Ensuring that staff should not have student contact details on their personal mobile phones; except for the specific duration of a school trip/visit;
u) Ensuring that student details are always taken from SIMS, and any new contact details obtained being passed to the school office for updating as may be appropriate;
v) Making students aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails, as part of the school's e- Safety and anti-bullying education programme.

7 Digital and Video Images

To prevent the inappropriate use of images of students within the School the following is observed:

a) Notification is given to parents that school, may publish photographs, video footage etc of students but that will ensure that images of their child may be used to only to represent the School, or, where appropriate, the University of Birmingham;
b) Photographs published on the Internet do not have full names attached;
c) Digital images and video of students are stored securely;
d) Pupils' and students' names are not used when saving images in the file names or in the <ALT> tags when publishing to the school website;
e) The School will avoid including the full names of students in the credits of any published school produced video materials or DVDs; or anywhere that they can be easily identified from photographs or videos
f) The Principal takes overall editorial responsibility for the website but delegate the operational day-to-day management to a named individual to ensure content is accurate and quality of presentation is maintained.
g) Uploading of information is delegated to individuals responsible for specified areas;
h) The School website complies with the Ofsted requirements;
i) Where other's work is published or linked to, the School credits the sources used and state clearly the author's identity or status;
j) The point of contact on the website is the main school address and telephone number, or occasionally individual School domain contact details. Home information or individual private e-mail identities will not be published;
k) Staff are made aware of the Acceptable Use of IT Policy (including a clause on the use of mobile phones / personal equipment for taking pictures of students) in induction;
l) Pupils and students are taught to be aware of the possible wide range of audiences and how images can be abused in their e-Safety education programme.

8 Cyber Bullying

8.1 The use of the Internet, text messages, e-mail, video or audio to bully another pupil or student or member of staff will not be tolerated.

8.2 Bullying can be done verbally, in text or images e.g. graffiti, text messaging, e-mail or postings on websites.

8.3 'Cyber bullying' is a form of bullying via communication technology like text messages, e-mails or websites. It takes many forms:

a) sending threatening or abusive text messages or e-mails,

b) personally or anonymously, making insulting comments about someone on a website, social networking site (e.g. Facebook) or online diary (blog/Twitter),

c) making, or sharing, derogatory or embarrassing videos of someone via mobile phone or e-mail (such as 'Happy Slapping' videos).

8.4 It should be noted that the use of ICT to bully could be against the law.

8.5 Abusive language or images used to bully, harass or threaten another, whether spoken or written (through electronic means), may be libellous and contravene the Harassment Act 1997 or the Telecommunications Act (1984).

8.6 The nature and consequences of cyber-bullying are addressed in PLAD lessons.

8.7 A range of strategies are recommended to support someone who is the victim of cyber-bullying.

9 Monitoring Arrangements

9.1 Appropriate monitoring arrangements in relation to all internet, e-mail and related services and facilities that it provides will be in place and the School will apply these monitoring arrangements to all users.

9.2 These arrangements may include checking the contents of, and in some instances recording, e-mail messages for the purpose of:

a) establishing the existence of facts;

b) ascertaining or demonstrating standards which ought to be achieved by those using the facilities;

c) preventing or detecting crime;

d) investigating or detecting unauthorised use of e-mail facilities;

e) ensuring effective operation of e-mail facilities, and;

f) determining if communications are relevant to the School, for example where an employee or student is off sick or on holiday.

9.3 The School may, at its discretion, apply automatic message monitoring, filtering and rejection systems as appropriate, and deny transmission of messages with content that is unacceptable in the terms of this policy.

9.4 These monitoring arrangements will operate on a continual and continuing basis, with the express aim of monitoring compliance with the provisions of the school's e-Safety policy and for the purposes outlined above as permitted by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000).

9.5 Disclaimer - the school may arrange for an appropriate disclaimer to be appended to all e-mail messages that are sent to external addresses from the school, in order to provide necessary legal protection.

10 E-Safety Education

10.1 An e-Safety programme will be provided for all pupils and students on:
- a) How to stay safe
- b) Social media
- c) Cyber bullying

10.2 At all Key Stages e-Safety forms a component of the assemblies.

10.3 As part of their induction, all new staff will attend an ICT workshop where e-Safety issues are discussed.

10.4 Staff are encouraged to view a CEOP film on the use of mobile devices.

10.5 All staff are required to read the e-Safety Policy and the Acceptable Use of IT Policy.

10.6 E-safety Information, advice and guidance will be provided for parents as part of their 'induction'.

10.7 The School website, newsletters and focussed communications will be used to provide updates concerning e-safety.

11 E-Safety Complaints

11.1 Complaints should be dealt with in accordance with the School's Complaints Policy and Procedures.

11.2 Complaints of cyber- bullying are dealt with in accordance with our Prevention of Bullying Policy.

11.3 Complaints related to safeguarding are dealt with in accordance with the Safeguarding Policy

11.4 The School will take all reasonable precautions to ensure e-Safety.

11.5 However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a School computer or mobile device.

11.6 The School cannot accept liability for material accessed, or any consequences of Internet access or ICT usage.

11.7 Investigation of Complaints
- a) The school will investigate complaints received from both internal and external sources, about any unacceptable use of ICT that involves the school IT facilities.
- b) External complaints will be addressed with reference to our Complaints Policy.
- c) The investigation of facts of a technical nature, e.g. to determine the source of an offending e-mail message, will be undertaken by the IT Team in conjunction with other departments as appropriate.

d) Where there is evidence of a criminal offence, consideration will be given to whether the issue will be reported to the police for them to take appropriate action. The School will co-operate with the police and other appropriate external agencies as required in the investigation of alleged offences.

11.8 In the event that the investigation of the complaint establishes that there has been a breach of the standards of acceptable use, then appropriate action will be taken.

11.9 In circumstances where there is assessed to be a breach of the standards of acceptable use, the schools will, as a first action, act promptly to prevent continuance or repetition of the breach, for example to withdraw any unacceptable materials.

11.10 This action will be taken in accordance with the normal managerial arrangements, and will typically involve liaison between the appropriate member(s) of the Leadership Team and the IT Team.

11.11 Subsequent action will be as described below:

a) Indications of non-compliance with the provisions of the e-Safety Policy will be investigated, as appropriate, in accordance with the provisions of the school's Disciplinary Procedures, as applicable to staff and students

b) Subject to the findings of any such investigation, non-compliance with the provisions of the e-Safety Policy will lead to appropriate disciplinary action, which could include dismissal on
the grounds of gross misconduct for staff members or exclusion for a student.

c) Furthermore, publication, accessing or storing of some materials may not only amount to a disciplinary offence, but also a criminal offence, in which case the issue will be reported to the police for them to take appropriate action

11.12 Complaints of cyber-bullying will be recorded and dealt with in accordance with our Prevention of Bullying Policy.

11.13 Complaints related to safeguarding will be are dealt with in accordance with the School Safeguarding Policy.

11.14 In the case of child pornography being found, the person or persons suspected should be immediately suspended and the Police will called on 0808 100 00 40.

11.15 Anyone may report any inappropriate, or potentially illegal activity, or abuse with or towards a child online, to the Child Exploitation and Online Protection (CEOP):
http://www.ceop.gov.uk/reporting_abuse.html.