UNIVERSITY OF BIRMINGHAM SCHOOL

University of Birmingham School

E-Safety Policy

March 2025

University of Birmingham School
E-Safety Policy

Review Frequency	Every two years	**Review date**	March 2023
Governing Committee Responsible	Teaching and Learning	**Next Due**	March 2025
Governor Approval (date)	8 March 2023	**Website**	Yes
Staff Responsible	C Townsend	**Date Produced**	

Contents	**Page**

At University of Birmingham School we refer to **Pupils** (who are in Years 7-11 and aged 11-16) and **Pupils/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 the School creates a safe ICT learning environment that includes three main elements:

a) An effective range of technological tools;
b) Policies and procedures 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 pupils, students, staff, and parents.

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

a) Prevention of Bullying Policy;
b) Behaviour and Exclusion Policy;
c) Safeguarding Policy;
d) Complaints Policy;
e) Assessment, Recording, Reporting Policy;
f) Acceptable Use of ICT Policy.

2 Key Principles

2.1 All pupils and 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 Pupils and 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 pupils and students can learn in a safe and secure environment, in and out of School.

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

3.3 To develop secure practice for pupils and students when communicating electronically.

3.4 To develop pupil and 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 Computer Science Team:

a) Ensure the School remains 'up to date' with E-Safety issues and guidance through organisations such as '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 on policy developments from time to time.

4.4 IT Services Team:

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

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

4.5 Teachers and Professional Services staff:

Are responsible for promoting and supporting safe behaviours in their classrooms and following School E-Safety procedures.

5 The security of the School's network:

This will be maintained by:

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

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 IT Services).

e) Not allowing pupils and students access to internet logs.

f) Using individual log-ins for pupils and 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 pupils and students only publish within appropriately secure learning environments such as their own closed secure log-in.

6 **The Internet**

a) University of Birmingham School recognises that access to the internet is an invaluable learning tool and vital for effective communication.

b) Safety and security risks are minimised through:

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

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

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

d) Informing users that internet use is monitored in the 'Acceptable Use of IT Agreement', and as part of our pupil/student induction process in Computer Science lessons;

e) Informing staff and pupils/students that that they must report any failure of the filtering systems directly to the IT Services 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 used as part of the teaching programme. A copy is kept on file, and this ensures parents/carers provide consent for pupils/students to use the internet, as well as other ICT technologies, as part of the E-safety acceptable use agreement form at the 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 the 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 available for pupils/students, staff and parents/carers;

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 School reserves 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 systems;

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

q) Ensuring staff only communicate with pupils/students via their designated School e-mail

account or designated School Class Charts 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, pupils/students on their personal social networking account or any other electronic device e.g. Facebook and suchlike;

t) Ensuring that staff should not have pupil/student contact details on their personal mobile phones; except for the specific duration of a School trip/visit and only then if necessary;

u) Ensuring that student details are always taken from Arbor, and any new contact details obtained being passed to the School office for updating as may be appropriate;

v) Making pupils/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 pupils/students within the School the following are observed:

a) Notification is given to parents/carers that the School may publish photographs and video footage of pupils/students but that it will ensure that images of their child may be used 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 pupils/students are stored securely;

d) Pupil/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 pupils/students in the credits of any published School produced video materials; or anywhere that they can be easily identified from photographs or videos

f) The Principal takes overall editorial responsibility for the website but delegates the operational day-to-day management to the Marketing and Communications Officer 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, the School credits the sources used and states 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 pupils/students) in induction;

l) Pupils/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**

a) This is recognised by the School as offensive communication by text, email, or image sent by telephone or the internet. It is a "method" of bullying, rather than a "type" of bullying. It includes bullying via text message; via instant messenger services and social network sites; via email; and via images or videos posted on the internet or spread via mobile phone. It can take the form of any type of bullying – i.e. technology can be used to bully for reasons of race, religion, sexuality, disability, and suchlike.

b) The use of the internet, text messages, e-mail, video, social media, Apps or audio to bully another pupil or student or member of staff will not be tolerated.

c) Bullying can be done verbally, in text or images e.g. graffiti, text messaging, e-mail, social media stories, postings on websites or circulating/sharing others' bullying comments, images, or text.

d) 'Cyber bullying' is a method of bullying via communication technology like text messages, e-mails, social media comments or websites. It takes many forms:

   a) Sending threatening or abusive text messages, emails or messages via an App e.g. WhatsApp, Snapchat, Instagram, TikTok,and suchlike.

   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, sharing, 'liking' or commenting on derogatory or embarrassing comments, threads, messages, images, audio or videos of someone via social media, mobile phone or e-mail.

e) It should be noted that the use of ICT to bully could be against the law. For example the Communications Act 2003 made it a criminal offence to send a malicious communication via social media.

f) Abusive language, images or communication used to bully, harass or threaten another, whether spoken or written (through electronic means), may be libelous and contravene the Communications Act 2003 or the Harassment Act 1997.

g) The nature and consequences of cyber-bullying are addressed in Learning for Life lessons and through our character education programme.

h) A range of strategies are recommended to support someone who is the victim of cyber-bullying. These are summarised in our Preventing Bullying Policy.

9 **Monitoring Arrangements**

a) 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.

b) 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.

c) 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.

d) 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).

**Disclaimer - the School will 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**

a) An E-Safety programme will be provided for all pupils/students on:

a) How to stay safe;

b) Social media;

c) Cyber bullying.

b) Staff are encouraged to view a range of training videos available through National College, our online training provider. Through this platform, staff can access all training videos created by National Online Safety.

c) All staff are required to read the E-Safety Policy and the Acceptable Use of IT Policy.

d) E-safety information, advice and guidance will be provided for parents/carers as part of their 'induction and as an ongoing part of our School commitment to online safety. All parents and carers will have access to National Online Safety, as a platform to help support their knowledge and understanding of online safety for their child(ren). Regular reminders will be shared with all families to ensure online safety remains a key focus of the School, and the families within our community.

e) The School website, newsletters and focused communications will be used to provide updates concerning e-safety, with a particular focus on the information and support shared through National Online Safety.

11 **E-Safety Complaints**

a) Complaints should be dealt with in accordance with the School's Complaints Policy and procedures.

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

c) Complaints related to safeguarding are dealt with in accordance with the Safeguarding Policy.

d) The School will take all reasonable precautions to ensure E-Safety.

e) 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.

f) The School cannot accept automatic liability for material accessed, or any consequences of internet access or ICT usage.

g) 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's 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 Services 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 and/or safeguarding incidents.

h) 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.

i) 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.

j) 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 Services Team.

k) 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 pupils/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 pupil or 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.

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

m) Complaints related to safeguarding will be dealt with in accordance with the School Safeguarding Policy.

n) In the case of child pornography being found, the person or persons suspected should be immediately suspended and the Police will be contacted without delay.

o) 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) service.

12 **Live-streaming lessons and video content**

a) Safeguarding is an integral principle of digital learning. The safety and welfare of learners is paramount and takes precedence over all other considerations.

b) Video conference or live-streaming a live lesson refers to the synchronous sharing of information or support in real time, not sharing a pre-recorded lesson, although similar safeguarding principles apply.

c) In this document a 'lesson' refers to delivery of a classroom lesson, perhaps with other children present in the classroom.

d) A 'session' refers to instances outside of a typical lesson with a learner perhaps for a one-one mentoring session or a small group catch up session.

e) At all times teachers should still continue to follow University of Birmingham School's 'Safeguarding Policy' and Keeping Children Safe in Education (KCSIE) guidance and any concerns about a child should be reported in the same way as soon as possible to a DSL.

f) To decide whether to use video conferencing, teachers must consider:
   - The availability of learners based on their individual circumstances e.g. are all learners available, are there enough laptops in the house if other live lessons are being shared.
   - The value of streaming live versus sending an asynchronous live lesson.
   - The ability to safeguard if streaming live with other pupils in the School classroom.

g) Pupil and student video and audio are disabled by default, they will not be able to change the video option.

h) Participants will only be able to access the live lesson using their School log-in and password - this is to ensure that no unauthorised people can access the lesson and no one can be anonymous.

i) Live lessons take place within Teams that are only accessible by pupils/students in that class.

j) The ability to present or screen-share is limited only to the teacher.

k) As a live stream recording constitutes personal data, the School must comply with its GDPR policy.

l) All recordings are saved within the Team channel, viewable only by the Team members and administrators, and are automatically deleted after 20 days.

m) The addendum to the Home School agreement for live-streaming is shared in advance with pupils/students and families. This sets out clear expectations for all parties and identifies actions if the agreement is broken (see appendix 1).

n) Sessions should only be delivered via Microsoft Teams from a School email account.

o) Cameras in the classroom should be face towards the teacher and away from any other pupils.
p) If a teacher isn't directly monitoring the on-line group then the audio and video of the group will be turned off.
q) Recording will not be used for any evaluation purposes.
r) When live streaming from home, teachers should continue to work in the same professional manner that they would assume in the classroom:
    - Sessions should only be delivered via Teams from a School email account.
    - No one-to-one sessions should take place (in exceptional circumstances, these will be agreed by the Principal in advance).
    - Adhere to suitable professional dress codes when in front of the cameras. Film in a living space, never a bedroom, and check the background is neutral; where possible, add a neutral 'blurred' filter.
    - Be conscious that remarks can be misconstrued and taken out of context so avoid unnecessary interactions.
    - End the session as soon as your supervision stops.
s) Setting out acceptable behaviours is essential. All pupils/students and families will receive an agreement beforehand, and in signing in to the lesson or session agree to abide by the guidance.
t) A common slide will be shown at the beginning of all online lessons reminding of expectations.
u) All pupils are automatically made 'attendees' and not 'presenters'.
v) The 'hands up' and 'chat' facility will be used to interact with pupils/students during the session.

Appendix 1

Home-School agreement: addendum for live-streamed lessons

Live lessons can be an important part of lesson delivery to supplement other types of learning when pupils/students or staff cannot be in School. In order to ensure all are safeguarded it is important that clear and robust guidance is in place for remote learning. By logging in to a live streamed lesson or session, parents, carers, pupils and students, and staff agree to the conditions below:

Staff will:

- Record all sessions for monitoring purposes when delivering a lesson in School. By logging in to the lesson, parents and carers agree to their child being recorded. All recordings will be held securely following the School's GDPR policy and deleted after 20 days.
- Follow the School's safeguarding policy at all times, and adhere to 'Keeping Children Safe in Education' guidelines.
- Keep all pupils/students as 'attendees' and mute video and audio, unless they are asking a direct question to a pupil.
- Schedule live lessons in advance on Teams and on ClassCharts to enable families to prepare the necessary IT.
- Disconnect any pupil or student who shows disrespectful or unsafe behaviour or who disrupts the learning of others.
- Disconnect the lesson once it has finished to prevent pupils/students being in a chat-room situation unsupervised.

Pupils and students will:

- Be punctual for lessons; because lessons may also be streamed live from classrooms that have other pupils/students present, no admittance is possible after the first five minutes.
- Be prepared with PREPP and an electronic device suitably charged, ready for learning.
- Seek to contribute to the lesson or session in a positive manner and not disrupt the learning of others.
- Actively engage where possible through the hands up or chat function.
- Not record or share any images from the lesson.

Parents and carers will:

- Provide a quiet space and appropriate IT as far as is possible, or request support from School if the relevant IT is not available.
- Ensure pupils/students are engaged and ready for learning.
- Feedback any safeguarding concerns immediately to the School's DSL or Principal.