UNIVERSITY OF
BIRMINGHAM
SCHOOL

University of Birmingham School

Acceptable Use of ICT Policy

March 2021

University of Birmingham School
Acceptable Use of ICT Policy – Pupils and Students

Review Frequency	Every three years		**Review date**	March 2021
Governing Committee Responsible	Teaching and Learning	**Approved(date)** 19 June 2017	**Next Due**	March 2024
Governor Approval (date)			**Website**	Yes
Staff Responsible	C Townsend		**Date Produced**	8 June 2015

Contents	Page
1. Purpose of Use	2
2. Definition of Acceptable Use	2
3. Equipment	2
4. Security	2
5. Passwords	2
6. Network Area	3
7. Data Sticks or USB Drives	3
8. Internet Use	3
9. Email	3
10. Right to Monitor	3
11. Privilege Versus Rights of Use	4
12. Penalties for Improper Use	5
13. Improper Use	5
14. Scope	5
15. Disclaimer of School Responsibility	5
16. Agreement	5

At 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 Purpose of Use

1.1 University of Birmingham School will offer all our pupils and students a wide variety of computing resources which are under constant review to ensure improvement and development.

1.2 Pupils and students are offered access to the School's network, internet and electronic mail (email).

1.3 Keeping our pupils and students 'safe' on the internet and supporting them to use the School network appropriately is one of our key responsibilities.

1.4 As a consequence we operate a '**Pupil and Student ICT Acceptable Use Policy**' (AUP) and anticipate that parents and carers will support us.

1.5 The 'Pupil and Student ICT Acceptable Use Policy' will be explained to all new learners during their first weeks in School and then reiterated annually.

1.6 Access to the University of Birmingham School network, internet, and electronic mail (email) will stop once students have left the School.

2 Definition of Acceptable Use

2.1 All pupils, students and their parents/carers must sign a copy of this 'Student ICT Acceptable Use Policy'.

2.2 The AUP explains what we consider to be acceptable use of our computer facilities and devices.

3 Equipment

3.1 All School computing equipment should be treated with care and respect.

3.2 Pupils and students must not attempt to move leads or change the setup of the device in any way.

3.3 Any damage to the equipment must be reported to a member of staff immediately.

3.4 Also, advice must be sought from a member of staff when using unfamiliar equipment.

4 Security

4.1 Security on any computer system is a high priority, especially when the system involves many users.

4.2 If a security problem is identified on the School network, email system or internet, a teacher and the IT Support Team should be notified immediately.

4.3 Pupils and students must not demonstrate the problem to other users.

4.4 Pupils and students must not use another individual's account.

5 Passwords

5.1 Passwords are strictly private.

5.2 Passwords should not be shared with anyone.

5.3 Pupils and students should not use anybody else's password.

5.4 The IT Support Team will re-set passwords which have become insecure.

5.5 Staff, pupils, and students should screen-lock PCs when away from them.

5.6 Passwords should be a combination of letters, numbers, and special characters, and be six characters or more.

5.7 Passwords should be changed regularly, and certainly when prompted by School systems to do so.

6 **Network Area**

Pupils and students are only permitted to navigate in the following areas of the School network:

a) Personal Data Area (My Documents)

b) Subject Departments

c) Filtered Internet

d) Personal OneDrive (via Office 365)

e) Appropriate Teams and SharePoint sites (via Office 365)

7 Data Sticks or USB Drives

7.1 These devices are only allowed to be used to remove and upload course work to the learner's own areas.

7.2 They are not to be used to run programs or games of any type.

7.3 Pupils and students should not store their only copy of any work on these devices; master copies must be kept on the network where it will be backed up daily.

8 Internet Use

8.1 Pupils and students should use the Internet to learn more about classroom topics, complete classroom projects, and to do homework.

8.2 The School recognises that some personal use by Sixth Form students is appropriate, and that occasional personal use that is brief in duration or infrequent is permitted, so long as it does not interfere with study, occurs in personal time, and is not otherwise prohibited by School policies or procedures.

8.3 If there is a question about whether the use of the internet is appropriate, ask the teacher or another person at the School designated to help decide whether a particular Internet use is appropriate.

9 Email

9.1 Pupils and students are responsible for all email sent from their account.

9.2 Pupils and students should use only appropriate language and tone when sending emails.

9.3 Pupils and students should not email large groups of users in 'chain-type' emails.

10 Right to Monitor

10.1 As part of the School's computing programme, we offer pupils and students filtered access to the internet.

10.2 Before the School allows pupils and students to use the internet, they must obtain permission from their parent/carer.

10.3 Various projects have proven the educational benefits of internet access, which enables pupils and students to explore thousands of libraries, databases, and bulletin boards – and conduct research.

10.4 They will also be able to exchange messages with other learners throughout the world.

10.5 It is the School's policy that every reasonable step should be taken to prevent exposure of pupils and students to undesirable materials/contacts on the internet.

10.6 It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable internet search yields unexpected results.

10.7 To reduce such occurrences, the School has adopted filtered access and has also installed the 'Impero' software suite.

10.8 This facility aims to stop pupils and students accessing sites deemed inappropriate for use at School, allows teachers to remotely monitor pupil and student access, and also provides a log of sites visited.

10.9 We believe that the benefits to pupils and students from access to the internet exceed any disadvantages.

10.10 However, as with any other area, parents and carers are responsible for setting and conveying the standards that their child should follow when using media and information sources.

10.11 The School therefore supports and respects each family's right to decide whether or not to agree to access.

10.12 During the School day, teachers will guide pupils and students towards appropriate material.

10.13 At home, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films, and radio.

10.14 Any inappropriate use is a violation of the AUP.

10.15 Any individual found to be in violation of this AUP will be subject to disciplinary action in line with the School's Behaviour Policy.

11 Privilege Versus Right of Use

11.1 The majority of our pupils and students will use the University of Birmingham School network, internet, and electronic mail (email) safely and sensibly and this document acts to increase awareness for all.

11.2 We take any infringement of the Pupil and Student ICT Acceptable Use Policy very seriously.

11.3 Any case reported will be thoroughly investigated and judged on an individual basis.

11.4 Pupils and students should expect serious sanctions to apply which may also result in either internet or network access being removed either temporarily or permanently.

11.5 The use of the School technology and access to the Internet are privileges and not rights.

12 Penalties for Improper Use

12.1 Penalties will include notifying parents and carers of the inappropriate use, suspension of user rights, and if necessary, revocation of user rights.

12.2 For malicious use, intended to cause distress, sanctions applied will include all measures up to and including exclusion, and will align with the School's other policies in place to promote good character, behaviour, and conduct – including the School's Behaviour Policy and Code of Conduct.

13 Improper Use

Examples of improper use by pupils might include:

a) Malicious damage of computing equipment – i.e. damaging keyboards, mice, or drives, damaged PC's, tablets or other expensive items;

b) Persistent attempts to circumvent the network security;

c) Copying information into assignments and failing to acknowledge the source (plagiarism and copyright infringement – we use specialist software to detect for this);

d) Cyber-Bullying - this can be in the form of emails, comments, blog entries, and chat rooms and can lead to exclusion from School;

e) Downloading materials or images not relevant to their studies, in direct breach of the School's acceptable use policy;

f) Misconduct associated with pupil and student log-ins, such as using someone else's password;

g) Incidents involving pupils and students using their own technology in School, such as leaving a mobile phone turned on or unauthorised use in class, sending nuisance text messages, or the unauthorised taking of images (still or moving) with a mobile phone camera;

h) Any attempt to run unauthorised personal applications (games or batch files);

i) Any attempt to gain access to restricted areas, and ;

j) Persistent attempts to circumvent the internet filter.

14 Scope

The content, reach, and expectations outlined in the policy apply in the context of hardware (including school owned and loaned equipment), software, and learner conduct – irrespective of whether learning is being undertaken on the School site – or remotely based at home or off-site.

In the circumstances of home-learning, especially where learning is synchronous via the internet and live-streaming, other agreements and expectations are in place to promote e-safety and safeguarding and must be followed appropriately. Details are outlined in the School's E-Safety policy.

15 Disclaimer of School Responsibility

The School is not responsible for any loss of data resulting from user negligence. This may include loss of coursework kept on student-owned USB devices.

16 Agreement

This policy must be agreed by both the pupil/student and parent/carer before a School based account can be created.