Bedford High School

A Specialist Business and Enterprise College

To Care To Learn To Achieve

Student and Staff E-Safety Policy

School Address	Manchester Road Leigh WN7 2LU
School Contact Number	01942 486386

Document control

Reviewed:	May 2018
Author/reviewer:	Rebecca Ramsden
Next review:	April 2019
Governing Committee:	FGB
Electronic copies of this plan are available from:	FROG VLN
Hard copies of this plan are available from:	HR, Facilities and Communications Manager
Public sector equality duty guidance considered	Yes
Date approved:	March 2017
Approved by:	Full Governing Body Committee

Changes History

Version	Date	Description	Changes
	May 2018	DSL name change, addition of 'Pastoral Managers' – generic term	Pg 2

Introduction

Bedford High School fully supports the importance and use of ICT. Inevitably, there are risks involved in the use of such technology and every effort is made to manage such risks and eradicate resulting negative behaviour from misuse.

The Internet is an unmanaged, open communications channel and many young people communicate regularly online with other users during evenings and weekends. Partly in response to this, students are educated on the benefits, risks and responsibilities of using information technology.

Students must learn that publishing personal information could compromise their security and that of others. E-Safety education makes clear to students, staff and visitors that the use of school equipment for inappropriate reasons is unauthorised. Reasonable actions and measures are put into place to protect users.

1.1 Aims

The E-Safety policy and associated procedures are in place to ensure young people use new technologies in a way which will keep them safe, without limiting their opportunities for creation and innovation.

The Internet and digital communications are an essential element in the 21st century for education, business and social interaction. The school computer system and Internet access is designed expressly for student use and will include filtering appropriate to the age of the students. Clear boundaries are set for the appropriate use of the computer system, the Internet and digital communications for staff and students.

1.2 Roles and Responsibilities

E-Safety is an important aspect of strategic leadership within the school and the head teacher and the governors have ultimate responsibility to ensure that practices are embedded and monitored. Additional responsibilities are highlighted in the table below:

Responsibilities	Staff Role	Named Person(s)
E-Safety Overview - Policy for E-Safety is written and regularly reviewed. - Policy complies to all regulations regarding E-Safety and safeguarding young people. - Oversees all staff involved in monitoring. - Following all policies related to E-Safety. - Reporting serious issues to the relevant authority. - Staff E-Safety CPD	Designated Safeguarding Lead E-Safety Coordinator	Mrs R Ramsden
E-Safety monitoring – technical - To provide updated anti-virus and filtering software on all computer access	Network Manager	Mr S Henderson

E-Safety monitoring - Delivery of e-safety assemblies / year group initiatives - Sanctioning for infringement of the Acceptable Use Agreeement	Pastoral Managers	Mrs K Eaton Mrs C Cottam Mrs Z Anders Mrs F Holland
Faculty Monitoring: - To ensure updated guidance is relayed and practiced within curriculum areas. - To discuss e-safety related issues and strategies, in relation to local and national guidelines with line managed staff.	Senior Leadership Team who line manage faculty leads	Mr P Shelton Mr P Mccaffery Mrs V Shakespeare Mr G Calwell
Student/Curriculum Guidance on Safe/Appropriate ICT use - Curriculum planning, monitoring and evaluation for KS3 and KS4	Teaching and Learning Coordinator for Computer Science and Media	Mr D Smedley
Teaching & learning using digital technologies - Ensuring e-safety when using technologies and communications	All teaching staff	All teaching staff

2.0 Teaching and Learning

Internet filtering software is used to ensure content is appropriate to the age of students. Students are taught about acceptable Internet use, given clear objectives for during curriculum time, and closely monitored through the use of Impero. Access levels are regularly reviewed to reflect the curriculum requirements and age of the students.

As mobiles/electrical equipment are not allowed in school, staff should not condone their use in lessons unless directed by the teacher. If a teacher wishes students to use their phones for a learning activity, the terms of use should be clearly displayed in the classroom (by for example cue cards) and students should be expected to stow their phones away securely before and after the activity.

Students have access to the school VLN, FROG, whereby they can upload and download work. This environment is a protected and monitored, and accessible from home and school.

2.1 Teaching and Learning – Access to inappropriate material

- If staff or students discover unsuitable sites, the URL (address), time, date and content must be reported to the Network Manager.
- Internet derived materials by staff and by students must comply with copyright law.
- Students are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Positive use of ICT is promoted.

The Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. To help manage online risk:

- Students are educated about the dangers of the misuse of social media and encouraged to explore issues relating to sharing personal information and data.
- Students are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed on how to block unwanted communications.
- All staff are made aware that bullying can take place through social networking.

2.2 The publishing of student's images or work

Photographs of students should not be published, online or otherwise, without the parent's or guardian's permission. A record of this is stored on SIMS.

2.3 Practices and procedures

- The school encourages the safe use of ICT for both staff and students and emphasises the importance of security and logging out of accounts.
- CPD and development of staff will be ensured.
- Positive use of ICT is promoted and updated in line with the developments of new technology.
- The school promotes methods for the reporting of cyber bullying in line with the Anti-Bullying policy.
- The school incorporates E-Safety advice to parents as part of parent's evenings/meetings.
- Reporting procedures are followed and records kept of all cyber bullying and/or sexting incidents in line with the Safeguarding and Anti-Bullying policies.

3. Behaviour for Learning

The Acceptable Use Agreement exists to provide clear expectations about ICT use in school (Appendix 1). The main premise of this agreement is that students will use the school computer network with responsibility.

If a student's use of the internet is deemed to be unsafe, unlawful or they are caught engaging in behaviour that may cause the school or other students harm, the student may be placed on contract, where they may have reduced or heavily supervised access to the internet. The contract will usually be followed with a sanction and/or referral to another agency who can support the student making the right choices on the internet. (Appendix 2).

3.1 How will information systems security be maintained?

- The security of the school information systems is reviewed regularly by the Network manager.
- Virus protection is installed on the network and updated regularly.
- Portable media must not be used without specific permission from the Network manager and a virus check.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked by the Network Manager.

3.1 How will e-mail be managed?

E-mail is an essential means of communication for both staff and students. E-mail should not be considered private and we reserve the right to monitor e-mail.

- All staff must sign the ‘Staff Common Agreement’, which includes acceptable use of email facilities.
- All students must sign the ‘Acceptable Use Agreement’, which includes acceptable use of email facilities.
- Only approved school e-mail accounts must be used on the school system.
- Staff and students must inform the Network Manager if they receive offensive/inappropriate e-mail (students would do this via their teacher).

3.2 How will Internet access be authorised?

- The school allocates Internet access for staff and students on the basis of educational need.
- All staff must read and sign the ‘Staff Common Agreement’ before using any school ICT resource. A record of this is held centrally.
- Parental permission for ICT use is required as part of our home-school agreement.
- To gain access to the internet, all students must agree to comply with the ‘Acceptable Use Agreement’.

3.2 How will risks be assessed?

The school will take all reasonable precautions to ensure that internet users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wigan Council can accept liability for the material accessed, or any consequences of Internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

3.3 How will e-safety complaints be handled?

The complaints procedure for parents/guardians is displayed on the school website.

- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.

3.4 Communicating E-Safety

- Internet access rules are displayed in all ICT classrooms.
- An annual E-Safety Week raises awareness of the importance of e-safety
- Students are informed that Internet use is monitored through Impero
- An E-Safety training programme is used to raise the awareness and importance of safe and responsible internet use.

- Useful resources and E-Safety websites are made available through the school website.

3.5 Staff and the E-Safety Policy

Staff are given opportunities to discuss and develop appropriate teaching strategies during faculty meetings and collaborative planning time. Staff must understand that the Internet misuse rules for Wigan council employees are quite specific.
If a member of staff is concerned about any aspect of their Internet use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

The induction of new staff should include:

- School E-Safety Policy and its importance explained.
- An explanation of network monitoring rationale and procedures.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- An explanation of the Staff Common Agreement.

3.6 How will parents' support be enlisted?

- Parents' attention will be drawn to the School E-Safety Policy on the VLN and school Web site.
- A partnership approach with parents will be encouraged.

Contacts and References

Child Exploitation & Online Protection Centre - www.ceop.gov.uk/
Virtual Global Taskforce – Report Abuse www.virtualglobaltaskforce.com/
Think U Know website - www.thinkuknow.co.uk/
Internet Watch Foundation - www.iwf.org.uk/
NSPCC - www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Childline - www.childline.org.uk/

Linked policies:

Anti-bullying policy
Safeguarding policy
Acceptable Use Agreement (Students)
Staff Common Agreement Form
IPad Acceptable Use Policy (Staff)
Guidance for Schools on Acceptable Usage of IT Policy (Staff)
Social Media Policy (Staff)