The Yehudi Menuhin School

P2.6 (ISI 7H) – E-SAFETY POLICY FOR PUPILS

Author :	Joanne Field – Head of Pastoral Care David Bruce – Designated Safeguarding Lead	29th January 2021 26th February 2021
Reviewed By:	Leadership Team	26th March 2021
Approved By :	Ben Gudgeon - Head	26th March 2021

Contents

Revision History

Revision	Paragraph Number	Revision
November 2017		
December 2020		Updated Format. Replaces previous policy 8.1. Policy updated to reflect latest developments in technology, use of devices, remote learning and KCSIE. Updated agreement form for pupils.

Abbreviations, Acronyms and Definitions

Abbreviation / Acronym	Definition
DSL	Designated Safeguarding Lead
INSET	In Service Education and Training
Leadership Team	Consists of: Headmaster, Director of Academic Studies, Director of Music, Bursar, Director of Development, Head of Pastoral Care & DSL.
Parents	Adults with parental authority for a child
Plagiarism	The act of taking someone else's work and passing it off as one's own.
PSHCE	Personal, Social, Health and Citizenship Education

Aim / Objective / Statement of Intent

1. This policy is intended to ensure:
    - that pupils will act responsibly and stay safe while using the internet and other digital technologies (including 3G, 4G and 5G) for educational, personal and recreational purposes;
    - that the School's systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
    - that pupils are protected from potential risk when using technology.
2. Wherever possible, the School will ensure that pupils have good access to digital technologies to enhance their learning. In return, the School expects pupils to agree to be responsible users.

Responsibilities

3. The Bursar is responsible for the School's technical provision and infrastructure, working with the School's IT providers to ensure that safeguards are in place to filter and monitor inappropriate content and alert the School to safeguarding issues. The Head and Assistant Bursar (Compliance & Estates), as joint Data Protection Officers, are responsible for ensuring that personal data is managed in line with statutory requirements.
4. The DSL will act as the School's E-Safety Co-ordinator and is responsible for:
    - ensuring that staff are trained in e-safety, through regular INSET and induction in this policy, as part of the School's wider safeguarding strategy, including:
        - sharing of personal data;
        - access to illegal / inappropriate materials;
        - inappropriate contact on-line with adults / strangers;
        - potential or actual incidents of grooming; and
        - cyber-bullying.
    - monitoring internet usage on the School network for misuse;
    - reporting incidents to the Head as necessary;

- liaising with the Head on any investigation and action in relation to e-safety incidents;
- compiling logs of e-safety incidents;
- advising on e-safety policy review and development; and
- ensuring that pupils receive age-appropriate guidance through the PSHCE programme (and any such other occasional training sessions as may be deemed appropriate) about the dangers of grooming, the accessing of inappropriate material, and the sharing of personal information or photographs, particularly on social networking sites. This will also include education on the dangers of extremism, in line with the School's commitment to the requirements of the Prevent Duty (see **P2.8 Prevent Duty Policy**).

5. The Director of Academic Studies is responsible for ensuring that the curriculum includes education and guidance for pupils on the safe use of technology and the provision and restrictions that apply to the use of technology in School.
6. The House staff will ensure that younger pupils have limited access to their mobile devices (and thus 3G, 4G and 5G provision).
7. Teaching and Support Staff will:
    - keep parents informed about any such guidance which is provided to pupils and seek their cooperation in helping the pupils to avoid putting themselves at risk whilst using such technology, particularly when online;
    - maintain their awareness of School e-safety policies and practices;
    - report any suspected misuse or problem to the Head or to the E-Safety Co-ordinator (DSL);
    - ensure that all digital communications with pupils / parents / carers/ fellow staff are on a professional level and conducted on school systems;
    - ensure, where relevant e-safety is recognised in teaching activities and curriculum delivery;
    - ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
    - monitor the use of digital technologies (including mobile devices, cameras etc. during school activities; and
    - ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

8. Pupils:

    - are responsible for using school digital technology systems in accordance with the school acceptable use policy;
    - will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
    - will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
    - are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying; and
    - will understand that the e-safety policy will include actions outside of school where related to school activities.

9. Parents / Carers:

    - will be advised of e-safety policies through parents' evenings, newsletters, letters, school website etc.;
    - will be encouraged to support the school in the promotion of good e-safety practice; and
    - should follow school guidelines on:
        - digital and video images taken at school events;
        - access to parents' sections of the school website / pupil records; and
        - their children's / pupils' personal devices in the school (where this is permitted).

10. Community Users / Contractors

    - Where such groups have access to school networks / devices, they will be expected to provide signed acceptance to abide by school e-safety policies and procedures.

Reporting

11. If concerns about e-safety arise which involve Child Protection issues they should be reported to the DSL immediately.
12. Other e-safety issues should be reported to the Head who will involve the Leadership Team, as necessary, to manage the issues.

13. If pupils raise issues concerning e-safety to pastoral or other staff, this should be raised at the weekly residential staff meetings which are chaired by the Head.

ICT Acceptable Use Policy Agreement – to be signed by pupils

I understand that I must use the School's systems in a responsible way to ensure there is no risk to my safety or to the safety and security of the School's systems or other users.

For my own personal safety:

- I will keep my password safe and secure: I will not share it, nor will I try to use anyone else's username or password. I understand that I should not write down or store a password where someone else might see it
- I will not disclose or share personal information about myself or others when on-line (includes names, addresses, email addresses, telephone numbers, financial details, etc.)
- I will report to the DSL (Ann Sweeney) or to any member of staff any unpleasant or inappropriate material or messages or anything that makes me feel worried or upset when I see it online.

I will act as I expect others to act towards me:

- I will not log on as another person or use another person's email address
- I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission
- I will not engage in plagiarism by copying other people's ideas or writings and presenting them as my own
- I will be polite and responsible when I communicate with others and not use strong, aggressive or inappropriate language
- In particular, I will not use language which is obscene, offensive or threatening in any way
- I will not engage in personal attacks on anyone or knowingly act in a way which might cause distress
- I will not post or send malicious information about any pupil, member of staff or the School
- I will not take or distribute any images or anyone without their permission
- In particular, I will not engage in any form of 'sexting'
- I recognise that any kind of 'sexting' or cyberbullying is not only against the School's rules, but may well be against the law and will be treated very seriously.

I recognise that the School has a responsibility to maintain the security and integrity of the technology it offers me to ensure the smooth running of the School:

- I will only use my personal devices in School if I have permission
- I will follow the rules set out in this agreement whenever I use school equipment or my own personal devices
- I will not try to upload, download or access any materials which are illegal or inappropriate or which may cause harm or distress to others
- I will consult a senior member of staff first before attempting to access any information which might break this Acceptable Use Policy (for example, research into extremism for a legitimate essay or project)
- I will not attempt to use any programmes or software to bypass the filtering or security systems in place
- I will not knowingly install spyware or any kind of hacking software

- I will not deliberately attempt to disrupt the system in any way, for example by knowingly distributing a virus
- I will not remove, tamper with, or cause damage to equipment belonging to the School or to others
- I will report any damage or faults involving equipment or software
- I will not attempt to install or store programmes of any type on any school device
- I will only use social media sites appropriate to my age
- I will use only the email address provided to me by the School when communication with members of staff

I understand that I am responsible for my actions both in School and out of School:

- I understand that the School has the right to take action against me if I am involved in incidents of inappropriate behaviour
- I understand that if I fail to comply with this Acceptable Use Policy Agreement I will be subject to disciplinary action; this could range from a warning or withdrawal of internet access to temporary or permanent exclusion from the School. Any breach of the law is likely to lead to the involvement of the Police.

Information Technology Acceptable Use Agreement (Pupils)

I have read and understood the rules in the Yehudi Menuhin School ICT Acceptable Use Policy Agreement.

I agree to follow these rules whenever:

- I use school systems and devices both in and out of School, whether on the School network or whilst accessing 3G, 4G or 5G
- I use my own devices in School (mobile phones, cameras, USB, gaming equipment, etc.)
- I use my own equipment out of School in a way that is related to me being a member of this School, e.g. communicating with other members of the School, accessing school email and website, etc.

NAME OF PUPIL	
SIGNATURE OF PUPIL	
DATE	