Flagship Learning Trust

Wright Robinson College

Wright Robinson College

E-Safety Policy

Approved: JANUARY 2020

Review Date: JANUARY 2022

Aims and Scope

Wright Robinson College aims to ensure that ICT will be used effectively to improve the learning outcomes and experiences of all students within the college.

The aim is that all stakeholders of Wright Robinson College will be committed to a shared responsibility towards achieving this aim. The intention is that ICT will be used to:

- Enhance the learning experience of Wright Robinson College students.
- Contribute to effective teaching and learning practice
- Allow efficient practices in administrative systems

In order to facilitate the aim, Wright Robinson College has policies and procedures in place to guide, support and safeguard those who utilise ICT.

Both students and staff at Wright Robinson College have access to computer resources and e-Learning materials. ICT is provided by an up-to-date Local Area Network (LAN) and a Wide Area Network (WAN) which ensure safe, secure and timely access to email, e-Learning resources, the Internet and educational software.

It is imperative that safeguarding is incorporated into best practice at Wright Robinson College and that all users are responsible and have a secure awareness of e-Safety. Therefore, the ICT policy documentation used at Wright Robinson College is intended to promote a positive ethos and behaviour regarding responsible ICT usage and Internet safety.

All staff members, both teaching and non-teaching will ensure that the policy set out below is implemented across all relevant areas of learning, teaching, administration and support. Wright Robinson College is fully committed to ensuring that the application of this acceptable usage policy document for ICT for students is non-discriminatory in line with the UK Equality Act (2010) and supports the Keeping Children Safe in Education statutory guidance. Further information and guidance can be found within the colleges Safeguarding and Child Protection policy.

Acceptable Use of ICT

Wright Robinson College provides computing resources for students use to enhance teaching and learning. This policy follows national guidelines in order to protect both the students and employees of Wright Robinson College.

e-Safety

- ICT users at Wright Robinson College, staff and students, must keep all personal information, private when using the internet. They should not share or send personal information (including name, address, email, bank details or telephone) from a Wright Robinson College computer.

- Students must only access those resources and services that they have been instructed / authorised by a member of staff to use.
- Students must inform a member of staff if they feel frightened or threatened by something they have accessed on the internet.
- Wright Robinson College believes it is essential for e-safety guidance to be given to the students on a regular basis. E-safety is embedded within our curriculum and our pastoral support programme.
- We understand the responsibility to educate our students on e-safety, teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Use of the Internet

- All Internet access is controlled by an Internet Content Filter which constantly monitors and logs all Internet activity.
- Restricted access of the Internet to students is controlled by the college IT management company
- The Internet is to be used only for educational purposes during teaching and learning time. Recreational activity during non-teaching and learning time is permitted only when authorised by a member of the teaching staff.
- Students should acknowledge and avoid plagiarism when researching information to produce pieces of work of their own.
- The Senior safeguarding Team and year offices are alerted to any websites and searches made by students that are unsuitable

Use of email

- Students must observe the polite and proper use of email at school and elsewhere. Students are prohibited from emailing or uploading to social networking sites any material that could cause offence or harm to other individuals and / or Wright Robinson College.
- Email use must be directly related to educational use. The forwarding of chain mail, spam, animations, hoaxes, virus warnings or nuisance emails is strictly forbidden.
- Any suspicious email must be treated with care and reported to a member of the teaching staff, Network Manager or IT service provider (Dataspire).

Use of social media, internet messaging and chat rooms

- Access to chat and social networking sites is strictly forbidden during school hours.

Cyber bullying

- Cyber bullying of any form will not be accepted or tolerated at Wright Robinson College. Wright Robinson will take immediate and serious action in line with the college's Bullying Policy and Behaviour for Learning Policy.
- Students and staff must ensure that all incidents of cyber bullying are reported to the relevant year team and or a member of the senior safeguarding team.
- Students are aware of the impact of Cyber bullying and are regularly advised and reminded on how to see help if they are affected by any form of cyber bullying. Students are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

Copyright

- The copyright of material and intellectual property rights must be respected. Students should never use material directly from an Internet source or CD and present it as their own work. Plagiarism sanctions will be enforced if students are found to have directly copied work.

Use of personal laptops and tablets on the school network

- Students are strictly prohibited from connecting to the Wi-Fi to gain access to the Internet at Wright Robinson College.
- Students are prohibited from the sharing of passwords with other students.
- Students may not use mobile devices in lessons unless specifically directed to do so by a member of staff.

Use of portable storage items

- Personal portable media devices should be used under the direction of the teacher for educational use only. Any files brought to school from a home computer (including homework) or downloaded from the Internet should be virus scanned before being used on a Wright Robinson College computer.
- Any misuse of portable storage will result in this privilege being removed.

Use of Staff Passwords / Computers

- The use of staff user names and / or passwords by other members of staff or students is strictly prohibited.

- Staff and students are expected to keep their passwords private. Staff and students are regularly reminded of the need for password security.
- Students must not be allowed to view documents that relate to private data of other students and must not be allowed to work on computers that allow them access to sensitive or official information, registers or records.

Taking Pictures on Mobile Devices

- The taking of pictures with mobile devices (such as mobile phones, iPads or iPods) by students within the Academy and its boundaries is strictly prohibited.

Playing of Games

- The use of school computers to play games, other than those games / activities with a specific educational purpose which are authorised by a member of staff, is strictly prohibited.

Data security

1. Students must not give their password to anyone else. All students are responsible for the safe keeping of their logon password which must be changed when prompted, to protect the college local network.
2. Students are responsible for all activities carried out during a session opened with their logon ID.
3. Students cannot download or install any applications.
4. Students must never delete the work of other students.
5. Remember, that all data on the network is the property of Wright Robinson College and can be viewed by authorised staff if necessary. This does not affect the student's privacy rights under the Data Protection Act.

Health and Safety

- Students should remember that computers are electrical equipment and therefore drinks must not be consumed in areas where there are laptops or computers.
- Students should avoid spending long periods of time on the computer without a break.

How to report misuse or accidental access of inappropriate materials

- If a student accidentally accesses unsuitable sites, the URL (address) and content must be reported to a member of staff immediately.

Monitoring by the school

- Students are personally responsible for the care of any ICT hardware provided and its use must comply with this policy.
- Students must make every effort not to waste resources, especially printer ink and paper. The ICT Department retain the right to monitor consumable usage and students may be billed accordingly if excessive resources are used through abuse of the system.

Sanctions for Misuse

- The use of computing resources is a privilege and any violation of the terms set out in this policy will result in access to the Internet and/or computing resources being restricted or withdrawn along with any further disciplinary measures deemed necessary.
- The use of computer systems without permission or for purposes not agreed by the college could constitute an offence under the Computer Misuse Act 1990.
- Students must not engage in any activity that could damage or threaten the functionality of any of the school's computing resources. Wright Robinson College will seek financial compensation for any malicious damage caused to ICT equipment.
- Sanction will be issued in the line with the colleges Behaviour for Learning Policy for any deliberate access to inappropriate material by students.
- Referrals will be made when appropriate to external agencies in line with the colleges Safeguarding Policy, if inappropriate information is accessed.
- A breach of policy may result in the temporary or permanent withdrawal of services.
- Policy breaches may also lead to legal proceedings.

Roles and Responsibilities (other than students)

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within the college. The day-to-day management of this will be delegated to a member of staff responsible for the whole college ICT provision (N Gallagher).

The Headteacher will ensure that:

- e-Safety training is provided to where appropriate students, all staff, leadership team and governing body, parents;
- The designated e-Learning person has had appropriate CPD in order to undertake the day to day duties;
- All e-Safety incidents are dealt with promptly and appropriately.

The Network Manager will:

- Keep up to date with the latest risks to children whilst using technology;
- Review this policy regularly and bring any matters to the attention of the Headteacher;
- Liaise with the IT managed service provider (Dataspire) and other agencies as required;
- Ensure ICT services maintain technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher;
- Any e-Safety incident is reported to ICT services and if required the Designated Person responsible for Child Protection.

Parents/Carers

- Wright Robinson College believes that it is essential for parents/carer to be fully involved in promoting e-safety both in and outside of the school and to be aware of their responsibilities and also where they can raise concerns and access support and guidance.
- Parents and carer are asked to read through and support the acceptable use agreement.
- Parents and carer are required to make a decision as to whether they consent to images of their student being taken and used in the public domain e.g. Website, social media and advertising.

Education and Training

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of the ICT programme;
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and within the PSHE curriculum. Students are taught through British Values and to prevent radicalisation.;
- Students will be taught whenever an opportunity occurs to be critically aware of the material/content they access on-line and be guided to validate the accuracy of information;
- Students will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the academies;

- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-safety training for all staff is included as part of Level 1 child safeguarding training;
- All new staff will receive e-safety training as part of their induction programme, ensuring they understand the E-safety Policy and Acceptable Use Policy.

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least every 2 years and in response to any e-safety incident to ensure that the policy is up to date and it covers all aspects of technology use within the school;
- Ensure e-safety incidents are appropriately dealt with and that the policy was effective in managing those incidents.
- Ensure that ICT security is detailed on the Trust Risk Register and reviewed regularly.