E-Safety Policy

(Written to comply with DfE statutory guidance – Keeping children safe in education, September 2024)

Date written/reviewed:		Oct 25
Written/reviewed by:		H Goodier
Approval:	Date:	
	Signed:	
	Position:	
Review due by:		Oct 26
Table of contents:		
Substantive changes since last review:		N/A

Introduction

Technology plays an important role at The Patch Project. It is often used within lessons as a central resource to help with the educational development of our students. Furthermore, it helps with the administrative side of our work with young people.

However, whilst the educational possibilities of using ICT are rapidly developing, all users of technology need to be alert and responsive to the potential dangers and risks associated with its use. These include:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

At The Patch Project , we understand the responsibility to educate our young people on e-safety issues; teaching them appropriate behaviour and skills to enable them to remain both safe and legal whilst using technology for learning or socially.

This policy aims to highlight some of the issues associated with ICT and provides guidance on how ICT should/could be used.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Education leader has ultimate responsibility to ensure that the policy and practices are embedded and monitored. All members of the Patch Project community need to be aware of the key people responsible for e-safety. At least one member of the Patch Project Team needs to have undertaken training by a recognised organisation to deal with issues relating to e-safety and to allow training to be given to staff.

There is an expectation that staff regularly access this policy on an annual basis. It is their duty to ensure they have an understanding of the issues and strategies at their centre in relation to local and national guidelines and advice.

This policy, supported by the Patch Project acceptable use agreements for staff, visitors and students, is to protect the interests and safety of the whole Patch Project community. It is linked to the following mandatory policies on safeguarding and child protection, and health and safety.

Social Networks

Facebook, X, Snapchat, Instagram, You Tube, online gaming and other forms of social media are increasingly becoming an important part of our daily lives. However, students can misuse social networks, including by sexually harassing their peers via their mobile and smart technology, sharing indecent images: consensually and non-consensually (often via large chat groups), and viewing and sharing pornography and other harmful content. In addition, there is an increased risk of online radicalisation, as terrorist organisations such as ISIL seek to radicalise young people through the use of social media and the internet.
Therefore, the use of social networks at The Patch Project is not allowed and young people taking part in lessons highlighting the risks when using the internet and social networks in their own time.

- Staff are not permitted to access their personal social media accounts using The Patch Project equipment during working hours. If staff are using The Patch Project equipment to access social media outside of work hours, they must be mindful of the fact that data will be stored locally within the device history, that they need to log out at the end of the session and that login details should not be auto-filled or remembered by the device.
- Students are not permitted to access their social media accounts whilst at The Patch Project on ANY device be it centre equipment or that of their own.

- Staff, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law.
- Staff should not befriend current students on social networking sites and best practise is to wait until that pupil is 19 before doing so (if necessary).
- Staff are not permitted to post any information or images regarding students or their centre on social media using their private account. Any posts for The Patch Project should be made on the relevant pages by the Education leader this can then be shared by others when available.
- It is recommended that all staff, who have private social media accounts change their user names to one where their identify can't be easily identified and privacy setting should be set to the maximum protection.

Mobile and Smart Technology

Students may bring mobile telephones or smart devices to the The Patch Project but they must be on silent or switched off and handed in to staff at the beginning of the school day. Students may be permitted to have their phones or devices back for a specified period within the lunch-break to check for messages, provided they are then handed back to staff until the end of the day. Students are not permitted to access social networks on their devices during this time and staff should provide an adequate level of supervision to ensure this does not happen. There should be no need for students to make or receive calls from their mobiles in the Centre – all phone calls should be made or received on the Patch Project phone.

Use of the Internet – including Filtering

Staff and students are able to access a wealth of information via the Internet to help with education/study. It is important though that the Internet is not used excessively and is well planned into the curriculum. The Patch Project provides students with supervised access to Internet resources Websites and their content are filtered by firewalls and Centres can add to the list of blocked sites flexibly and quickly.

Staff should preview any recommended sites before use to check that they work on the school system and are appropriate, including checking that they do not contain any terrorist or extremist material.

Raw image searches are discouraged when working with students and key search terms are provided to students.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents/carers will be advised to supervise any further research.

All users must observe copyright of materials from electronic resources.

The Internet should be used primarily for educational purposes. Where students are given permission to use the Internet recreationally, close supervision must be given to the sites they are visiting and content they are viewing.

Monitoring

Authorised ICT support staff may access ICT equipment that is owned / leased by the school at any time with prior notice.

In certain circumstances the Education leader may instruct the service provider to monitor, intercept, access, inspect, record and disclose e-mails, instant messaging, internet/intranet use and any other form of electronic communication involving any student or employee, without consent, to the extent permitted by law.

Occasions where this may be necessary include

- Confirming or obtaining school business related information
- Confirm or investigate compliance of school standards, policy and procedures
- Quality control or training purposes
- Prevent or detect crime
- Child protection

All monitoring, investigative and surveillance work should be conducted by authorised ICT staff and comply with the Data Protection Act 1998, Human Rights Act 1998, Regulation of investigatory Powers Act 2000 and the Lawful Business Practises Regulations 2000.

Acceptable Use Agreements

Each year, ALL staff employed at the Centre shall undertake some training with regards to e-safety. As part of this training, all employees should sign an Acceptable Use agreement and this must be held by the Education leader.

All students should take part in one dedicated lesson at the start of the year (or when they start at the centre) where e-safety is addressed and students re-sign an Acceptable Use Agreement.

A copy of the staff, young people and parent agreements can be found in the appendices of this policy.

Parents/carer should be alerted to the e-safety policy during the referral interview, through the *referral form* and it should be made available as a hard copy or electronically if requested. The e-safety policy and additional information related to e-safety is accessible from the Patch Project website. Parents should sign the AUP and read the e-safety policy during the referral interview before their young person starts at The Patch Project. They should also be aware of and give consent to any guidance for online distance learning. E.g. All meeting will be recorded.

Cross Curricular E-Safety

ICT now plays a key part in the education of students. ICT is used widely for research and to enhance the quality of work produced by students. It is important that teaching and learning incorporates the use of ICT and that when planning and delivering lessons using ICT, matters relating to e-safety are considered by all staff.

Staff Training

Training will be provided annually to all staff as part of the introduction to the new school year. This will be focussed on keeping students safe and managing risk. Regular information on e-safety will be provided to staff to keep staff abreast of developments. Over the school year, there may be opportunities for staff to attend additional training events. Information about these will be published when available.
All staff will review the acceptable use agreement on an annual basis and sign the document to acknowledge their professional responsibilities in relation to ICT in general. New staff starting midyear will need to sign this as part of their induction.

Use of Digital Images and Video

Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is not always appropriate to take or store images of any member of the Patch Project community or public, without first seeking consent and considering the appropriateness.

- Not all parents' give permission for photographs of students to be taken. This information can be found on student records and must be adhered to as there are often safeguarding reasons why photographs should not be taken and used.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Education leader.
- Where digital images / photographs are used and shared publicly, students' first names only should be used.
- For the protection of all involved online lessons will be recorded and they will be kept in line with our GDPR requirements.

Misuse of ICT

- Complaints of Internet Misuse must be reported and dealt with by the Education leader.
- Any complaint about staff misuse should be directed to the Education leader.
- Any issue of a child protection nature should be referred in the usual manner to the Designated Safeguarding Lead.

Reviewing Online Safety

The Education leader will carry out an annual review of our approach to online safety, which will be supported by an annual risk assessment that considers and reflects the risks our students face. Issues arising from this will be incorporated into written policies and procedures and addressed during annual staff training.

Appendix A: XXXX E-Safety – Staff Code of Conduct for ICT / AUP

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult The Patch Project 's e-safety policy for further information and clarification.

- ☐ I understand that it is a criminal offence to use ICT system for a purpose not permitted by its owner.
- ☐ I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for The Patch Project business.
- ☐ I understand The Patch Project information systems may not be used for private purposes without specific permission from the Head of Centre.
- ☐ I understand that my use of The Patch Project information systems, internet and email may be monitored and recorded to ensure policy compliance.
- ☐ I will respect security and I will not disclose any password or security information to anyone other than an authorised system manager.
- ☐ I will not install any software or hardware without permission.
- ☐ I will ensure that personal data is stored securely and is used appropriately, whether in The Patch Project , taken off the premises or accessed remotely.
- ☐ I will respect copyright and intellectual property rights.
- ☐ I will follow all online/distance learning /check in procedures as outlined in the e-safety policy
- ☐ I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead.
- ☐ I will ensure that electronic communications with students including email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- ☐ I will ensure that my use of ICT systems privately (e.g social networking, text messaging) will not crossover with my ICT use professionally by protecting my social networking profiles from public view, and not giving out personal contact information **I will not add current students as friends on social networking sites, and will take care to ensure that any comments about The Patch Project activities are appropriate and professional.**
- ☐ I will not post any information or images regarding students or The Patch Project on social media using my private account.

The Patch Project may exercise its rights to monitor the use of the information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the information systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed:..... Print name:……..... Date: .....

Student Acceptable Use Agreement

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the Patch Project IT equipment for appropriate activities and learning and am aware that the school can monitor my internet use.

2. I will not access any of my social media accounts on any device while at The Patch Project , including devices owned by The Patch Project and those that belong to me.

3. I will not bring files into The Patch Project that can harm the network or be used to circumvent security tools.

4. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.

5. I will keep my logins, IDs and passwords secret and change my password regularly.

6. I will use the Internet responsibly and will not visit web sites that are inappropriate for the school or my key stage.

7. I will only e-mail or contact people I know, or those approved as part of learning activities.

8. The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and The Patch Project .

9. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.

10. I will not give my personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.

11. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room.

12. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.

13. I am aware that some websites, games and social networks have age restrictions and I should respect this.

14. I am aware that my online activity at all times should not upset or hurt other people. This includes not taking or sharing any images, including of staff or other students which could be used to offend or deliberately hurt or upset them. I'm aware that procedures are in place to protect staff and students from this activity and that action will be taken against anyone who disregards this agreement.

I have read, understood and accept the Acceptable Use Agreement for ICT.

Signed:..... Print name:……..... Date: .....