Maple Medical PRU E Safety Policy

The e-Safety Policy relates to other policies including those for Acceptable Use, social media, anti-bullying and for child protection
The Centre has appointed an e-Safety coordinator who is the Head teacher Kath Formby
Our e-safety Policy has been written by the Centre, using government guidance. It has been agreed by senior management and the Management Committee

E-mail and Internet use

The Internet is an essential element in 21st century life for education, business and social interaction. The centre has a duty to provide pupils with high-quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils

Internet Use

The centre's Internet access is provided by DMBC and complies with DCSB (Doncaster Children's Safeguarding Board) requirements for safe and secure access. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. The Hospital School internet access is provided by DRI.
We have the facility to block any Inappropriate sites that may get through the filtering software
When appropriate, pupils are given Internet access at home via a laptop in order for them to complete homework or to access sites for research. Parents/ carers and pupils sign up to an Acceptable use policy before they are allowed to take this home.
Clear boundaries will be set for the appropriate use of the internet and digital communications and discussed with staff and pupils
Pupils will be educated in the effective use of the internet in research including the skills of knowledge location, retrieval and evaluation

E-mail
Pupils do not currently have access to school email accounts, if this is to change then the following rules apply:

- Pupils may only use approved e-mail accounts on the school system
- They must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Pupils in the Hospital School sometimes use their school email for hospital school staff to email work to them using their approved Maple email address

Managing Internet Access
Information system security
School ICT system security will be reviewed regularly.
Virus protection will be installed and updated regularly.
Security strategies will be discussed with the Local Authority.
For the hospital school, security strategies will be discussed with the hospital as well as the LA

Publishing pupils' images and work
Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.
Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils or babies are published on the school Web site.
Work can only be published with the permission of the pupil and parents/carers. We do not publish images of looked after children.
At the hospital school we have to use the DBTH specific forms for photographs to be published.

Use of mobile technology
Staff may be issued with a school phone where contact with pupils or parents/carers is required
Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
The use by pupils and staff of cameras in mobile phones is discouraged
In the hospital school and the rest of Maple, we are not allowed to take photographs on mobile phones. All photos have to be taken on a camera or iPAD registered to the school and in the case of the hospital school, have to be deleted immediately.

The School Website
Staff or pupil personal contact information will not be published. The contact details online will be the school offices.
The head teacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
The senior management team should note that technologies such as mobile phones with mobile Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Assessing risks
The centre will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the centre nor DMBC can accept liability for any material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints
Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the head teacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
Pupils and parent/ carers will be informed of the complaints procedure.
Discussions may be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues

Staff and the e-Safety policy
All staff will be given access to the School e-Safety Policy and its importance explained.
Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must always take care to maintain a professional relationship.

Introducing the e-safety policy to pupils
E-Safety rules will be posted in all rooms where computers are used. Pupils will be informed that network and Internet use will be monitored. A programme of training in e-Safety will be developed and delivered

Introducing the e-safety policy to parents and carers
Parents and carers attention will be drawn to the school e-safety Policy in newsletters, the school brochure and on the school Website. Parents/ carers will be given the opportunity to access training after school.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the general Data Protection Regulations (GDPR) May 2018
A Privacy Notice (Data Protection Bill 2018) letter is sent to parents/ carers on admission of new pupils advising them how we use and protect data at Maple

All staff, management committee members and pupils have secure e-mail addresses

Date of Policy – March 2022

Date of Review – March 2024

Head teacher signature ……

Management Committee signature…….