THE DEANES

E-Safety Policy

Adopted:

Reviewed:

June 2023

E-Safety Policy

Contents

June 2023

Introduction

At The Deanes, our 6 Promises state our vision for the school, and encapsulate our ‘iMatter’ ethos. Each and every one of our students can feel happy, respected and known as an individual (Promise #1).

Ensuring students are safe in school, but also that they are able to protect themselves from harm, is of paramount importance. Students need to be educated to make safe but effective use of the considerable learning potential inherent in information and communication technology (ICT).

This e-safety policy is therefore concerned primarily with safeguarding and educating students to navigate these risks and to be in a position to use new technology safely and responsibly to maximise their learning.

AIMS

Our aim is to do all we can to protect and safeguard the wellbeing of all our students and to educate them to be risk-literate and in a position to harness the potential of new technology for their learning and in their future lives.

Children and young people have a fundamental right to be protected from harm. Our students have the right to expect us to provide them with a safe and secure environment and we recognise that the protection and education of our students is a shared responsibility.

PRINCIPLES

- Our work around e-safety must ensure students are safe and secure in school in relation to the potential dangers posed by new technologies.
- Our work must challenge the normalisation of dangerous behaviours, eg ‘sexting’ or youth produced imagery.
- In safeguarding students, we must not disempower students to be able to make safe and responsible choices.
- Appropriate sanctions need to be employed beyond preventative approaches, where an action or behaviour is deemed counter to our Behaviour Policy.
- Our work is focused primarily on students, but in accepting our responsibility, we must ensure that staff are aware of the risks and are proactive in tackling e-safety, that Governors hold the school to account through monitoring and evaluating our actions, and that parents/carers are also empowered to provide support.
- Our work on e-safety relates to our overarching Safeguarding Policy and practice, as well as our approach to the curriculum and teaching and learning (Promise #1).
- We will liaise with external agencies, including the Police and CEOPS, whenever appropriate to do so.

PRACTICE

(A) EFFECTIVE E-SAFETY EDUCATION

Students:

- E-safety is a cross-curricular theme which is currently explored explicitly in numerous parts of the curriculum, including the following:

Computer Science	Key Stage 3
RSHE	Key Stage 3 and 4
Tutorial	Key Stage 3 and 4

- Assemblies are delivered to all students on an annual basis to raise awareness and explain where students can access further support.
- Information regarding safety is provided on our website for student/parent information.
- Students have an ICT Acceptable use policy
- Bullying in relation to e-safety (cyber bullying) is noted on the school's discrimination log and appropriate sanctions issued and support provided where appropriate.
- Students deemed vulnerable/at risk from e-safety issues are supported/guided by our pastoral team to support their wellbeing.
- Sanctions will be applied as required in line with the school's Behaviour Policy.
- Some students receive additional external support from appropriate agencies

Staff:

- **Our Designated Safeguarding Lead (DSL)** is the Designated E-safety co-ordinator, working in conjunction with the Trust ICT Lead and Mr Desi McKeown (Headteacher).
- All staff are expected to address e-safety issues where appropriate in the course of their work.

Governors:

- Governors have ratified this e-Safety Policy and its effectiveness will be reviewed periodically.
- Governors receive updates on cyber-bullying via the Headteacher's termly report to Governors. E-safety progress is reported to Governors on a termly basis in the Headteacher's report.
- Gill Baynes, as Safeguarding Governor, is the nominated e-Safety Governor who liaises with our Designated Safeguarding Lead on a termly basis.

Parents:

- Parent workshops are provided by the school when available.
- Additional information is available for parents on our website, offering advice and additional sources of information/support.
- New or useful information is shared with parents regularly via our weekly Newsletter.
- Our Pastoral Team provide additional support to families encountering issues/concerns.

(B) ENSURING A SECURE E-SAFETY ENVIRONMENT IN SCHOOL

Students:

- Students are expected to follow the ICT Acceptable Use Policy as distributed at the start of the academic year.
- Students are given information about how to report any e-safety.
- Each computer within the school will display an Impero icon so that students may share concerns.
- Mobile phone devices are not permitted in school and if they are seen, they will be confiscated.

Staff:

- All e-safety issues are monitored and should be dealt with promptly and appropriately. Staff are expected to report any concerns to our Designated Safeguarding Lead immediately via MyConcern.
- Staff are expected to use ICT responsibly with regard to our Staff Code of Conduct. In particular, the 'Code of Conduct Policy' should be consulted re: expectations on staff use of ICT.
- The ICT team constantly reviews that appropriate technical e-safety measures are in place, with appropriate filters to safeguard students. This links to our work re: PREVENT to combat the risk of radicalisation in accordance with government guidelines. PREVENT concerns will be dealt with according to our Safeguarding Policy.
- Staff receive online safety training annually and are expected to be aware that social media is increasingly being used to radicalise and recruit young people to commit acts of terrorism.
- Staff have completed a cyber security training course.
- The ICT team constantly review the overall security of the network, including appropriate anti-virus software - Microsoft Defender.
- Our filtering levels are monitored regularly to prioritise safety but enable learning resources to be accessed where needed.
- Staff will not take or transmit images/sound files of students, colleagues and/or their work on a personal mobile device.
- Our filtering system automatically notifies the DSL immediately if inappropriate searching is detected. Any concerns raised are flagged to the appropriate member of staff so that action can be swiftly undertaken.