Our e-safety policy 2021

The use of technology has become a significant component of many safeguarding issues: child sexual exploitation; radicalisation; sexual predation – technology often provides the platform that facilitates harm. This policy should be read in conjunction with Keeping Children Safe in Education 2021.

This policy and the procedures that it underpins apply to all staff, including senior managers, paid staff, volunteers and sessional workers, agency staff, students and anyone working on behalf of Oaklands School and intends:

- to protect children and young people who receive Oaklands School services and who make use of information technology as part of their involvement with us;
- to provide staff and volunteers with the overarching principals that guide our approach to e-safety;
- to ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use information technology.

We recognise that:

- The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk. For the purposes of this policy, "inappropriate content" refers to any of the following, broadly construed:
    - **content**: being exposed to illegal, inappropriate or harmful material; for example: pornography, fake news[1], racist or radical and extremist views
    - **contact**: being subjected to harmful online interaction with other users; for example, adults posing as children or young adults, obscene or threatening communications;
    - **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying
    - **Commerce**: Risks such as online gambling, inappropriate advertising phishing and financial scams.
- the welfare of the children/young people who come into contact with our services is paramount and should govern our approach to the use and management of electronic communications technologies;
- all children, regardless of age, disability, gender, racial heritage, religious belief, sexual orientation or identity, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to e-safety

[1] See the House of Commons DCMS Committee's "Disinformation and 'fake news': Interim Report", pg. 7 for a robust definition of what constitutes 'fake news'.

- the use of information technology is an essential part of our lives; it is involved in how we as an organisation gather and store information, as well as how we communicate with each other. It is also an intrinsic part of the experience of our children and young people, and is greatly beneficial to all. However, it can present challenges in terms of how we use it responsibly and, if misused either by an adult or a young person, can be actually or potentially harmful to them.

We will seek to promote e-safety by:

- Appointing an e-safety coordinator;
- Developing a range of procedures that provide clear and specific directions to staff and volunteers on the appropriate use of ICT;
- Putting appropriate technical measures in place to ensure that inappropriate content (as defined above) is blocked – please see below for further details.
- Supporting and encouraging the young people using our service to use opportunities offered by mobile phone technology and the internet in ways that keep themselves safe and shows respect for others;
- Supporting and encouraging parents and carers to do what they can to keep their children safe online and when using their mobile phone, iPod, tablet and game consoles;
- Incorporating statements about safe and appropriate ICT use into the codes of conduct both for staff and volunteers and for children and young people;
- Developing an e-safety agreement for use with young people and their carers;
- Use our procedures to deal firmly, fairly and decisively with any examples of inappropriate ICT use, complaints or allegations, whether by an adult or a child/young person (these may include breaches of filtering, illegal use, cyber bullying, or use of ICT to groom a child or perpetrate abuse);
- Informing parents and carers of incidents of concern as appropriate;
- Reviewing and updating the security of our information systems regularly;
- Delivering information security training to staff and service users, to ensure they follow basic best practices such as not divulging passwords, creating suitably secure passwords, and are aware of information security risks such as phishing.
- Using only official email accounts provided via the school for school business, and monitoring these as necessary;
- Ensuring that the personal information of staff, volunteers and service users (including service users' names) are not published on our website;
- Ensuring that staff accounts on any system only have access to the information (e.g. files, records) that they require to perform their duties, to minimise the risk of data loss;
- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given

- Any social media tools used in the course of our work with children, young people and families must be risk assessed in advance by the member of staff wishing to use them;
- Providing effective management for staff and volunteers on ICT issues, through supervision, support and training;
- Examining and risk assessing any emerging new technologies before they are used within the organisation.
- Ensuring that staff are aware of the guidance provided by the UK Safer Internet Centre on how to keep young people safe online.

Internet filtering:

- Oaklands School's Internet connection is provided by the London Grid for Learning (LGfL), a supplier that exclusively serves schools and colleges. All Web access is filtered by the LGfL – it is impossible to configure a device to bypass the filtering[2].
- The LGfL has a baseline filter, which blocks a large range of inappropriate content. Specific Web addresses can be blocked or unblocked by the school's IT team (barring some that cannot be unblocked for legal reasons). Social media sites such as Facebook, Twitter and Instagram are blocked by default.
- All web access is logged for 28 days, and these logs can be interrogated by the IT team on request.
- Staff can request that Web sites are blocked or unblocked by using the school's IT helpdesk system – the IT team will review the request and take appropriate action All blocking or unblocking requests *must* be logged in the helpdesk – no request will be actioned by IT without a ticket. If they are at all unsure about a site's suitability, they will request input from the Designated Safeguarding Lead or their deputy.
- The IT team will also endeavour to keep the filter up to date to deal with emerging threats.
- Staff will be made aware that **no filtering system can catch everything**, and that they must examine any site they intend to use with service users themselves before using it.

ICT monitoring:

- Oaklands School uses a PC monitoring solution called Impero Education Pro to monitor what service users access.
- Should an attempt be made to access an inappropriate Web site, or an inappropriate search be made, the school's IT team will be notified, and they will then pass the message on to the Safeguarding team.

[2] In technical terms, it uses what is called a **transparent proxy**. All connections are routed through the LGfL's filtering systems.

- All Internet access is also logged by Impero, which provides a more granular log than the LGfL. For example, Impero's log can determine on which PC content was accessed, whereas the LGfL will simply say what was accessed at what time.

The name of our e-safety coordinator is **Mairead Standring**.
She can be contacted at **Oaklands School** on 0208 560 3569.
We are committed to reviewing our policy, procedures and good practice annually.