

## Addendum to CP and Safeguarding Policy – February 2024

### Online safety and the use of mobile technology

We recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues.

To address this, our school aims to:

- Have robust processes (including filtering and monitoring systems) in place to ensure the online safety of pupils, staff, volunteers and governors.
- Protect and educate the whole school community in its safe and responsible use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)
- Set clear guidelines for the use of mobile phones for the whole school community.
- Establish clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate

### The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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.

To meet our aims and address the risks above, we will:

- Educate pupils about online safety as part of our curriculum. For example:
  - The safe use of social media, the internet and technology
  - Keeping personal information private
  - How to recognise unacceptable behaviour online
  - How to report any incidents of cyber-bullying, ensuring pupils are encouraged to do so, including where they're a witness rather than a victim
- Train staff, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying, the risks of online radicalisation, and the expectations, roles and responsibilities around filtering and monitoring. All staff members will receive refresher training as required and at least once each academic year
- Educate parents/carers about online safety via our website, communications sent directly to them and during parents' evenings. We will also share clear procedures with them, so they know how to raise concerns about online safety.
- Make sure staff are aware of any restrictions placed on them with regards to the use of their mobile phone and cameras, for example that:
  - Staff are allowed to bring their personal phones to school for their own use, but will limit such use to non-contact time when pupils are not present.
  - *Staff will not take pictures or recordings of pupils on their personal phones or cameras or any other electronic devices capable of imaging and sharing as noted in the [Staff Code of Conduct](#) and [BDMAT IT policy](#)*
- Make all pupils, parents/carers, staff, volunteers and governors aware that they are expected to sign an agreement regarding the acceptable use of the internet in school, use of the school's ICT systems and use of their mobile and smart technology.
- Explain the sanctions we will use if a pupil is in breach of our policies on the acceptable use of the internet and mobile phones.
- Make sure all staff, pupils and parents/carers are aware that staff have the power to search pupils' phones, as set out in the [DfE's guidance on searching, screening and confiscation](#)
- Put in place robust filtering and monitoring systems to limit children's exposure to the 4 key categories of risk (described above) from the school's IT systems. Please see [BDMAT IT policy](#)

- Carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks faced by our school community.
- Provide regular safeguarding and children protection updates including online safety to all staff, at least annually, in order to continue to provide them with the relevant skills and knowledge to safeguard effectively.
- Review the child protection and safeguarding policy, including online safety, annually and ensure the procedures and implementation are updated and reviewed regularly.

This section summarises our approach to online safety and mobile phone use. For full details about our school's policies in these areas, please refer to our [Staff Code of Conduct and BDMAT IT policy](#)

### Childcare Disqualification

All staff working in Early Years, and children under five years of age in school hours and children under 8 years of age in Wrap-around provision are required to complete a Childcare Disqualification declaration.

### Staff taking medication/other substances.

Staff members must not be under the influence of alcohol or any other substance which may affect their ability to care for children.

If a practitioner is taking medication which may affect their ability to care for children, they should seek medical advice. Practitioners must only work directly with children if the medical advice received confirms that the medication is unlikely to impair that person's ability to look after children properly. Staff must inform their line manager that they are on medication that may affect their ability to care for children so adequate support can be implemented. All medication on the premises must be stored securely, and out of reach of children, at all times.