E-Safety Policy

Owston Park Primary Academy

Introduction

The use of computers and other technologies with online access are an integral part of the world today and has become more easily accessible for all. Learning how to use them safely, with the least risk, is a key life skill. At Owston Park we recognise that pupils are entitled to a broad and balanced computing education that addresses E-safety as a vital part of that curriculum delivery. The purpose of this policy is to state how the school intends to match this provision including while implementing remote education.

Aims

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers our school to protect and educate pupils, parents/carers, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. The E-safety curriculum that is delivered to the children at Owston Park is through Common Sense Education. This is taught to every child in school on a three week rolling programme alongside PSHE and Life Skills.

The school's aims for E-safety are to ensure:

- All pupils can recognise dangers while online, in a range of contexts.
- All pupils know how to keep themselves safe while online.
- All pupils know who to talk to if they are uncomfortable or concerned about something online.
- All pupils become responsible online citizens, who are respectful online.

The National Curriculum for Computing aims to ensure that all pupils:

- **Key Stage 1:** Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- **Key Stage 2:** Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-safety of individuals and groups within the school.

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including E-safety) of members of the school community.
- The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.

E-Safety Coordinator/Officer:

Miss J Scarfe

- Takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- Provides advice for staff.
- Receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments.
- Reports regularly to Senior Leadership Team.

Network Manager / Technical staff:

Mrs V Stinson, Miss J Scarfe, Sam Drury - Wavenet

Are responsible for ensuring:

- That the school's computing infrastructure is secure and is not open to misuse or malicious attack.
- The school's computing infrastructure has appropriate and strong filtering and monitoring procedures and protections in place.
- That the school meets the E-safety technical requirements outlined in any relevant National or Local Authority E-Safety Policy and guidance.
- That users may only access the school's networks through a properly enforced password protection policy e.g. MFA.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of E-safety matters and of the current school E-safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP).
- They report any suspected misuse or any other problem to the E-Safety Coordinator /Headteacher/Member of SLT.
- Designated Safeguarding Lead: Mrs V Stinson, Deputy: Mrs J Semley.
- They are trained in E-safety issues and are aware of the potential for serious child protection issues to arise from:

- sharing of personal data.
- access to illegal/inappropriate materials.
- inappropriate on-line contact with others.
- potential or actual incidents of grooming and abuse.
- cyber-bullying.

Students/pupils:

- Are responsible for using the school computing systems and mobile technologies in accordance with the Student/Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (at KS1 it would be expected that parents/carers would sign on behalf of the pupils).
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Parents/Carers:

The school will take every opportunity to help parents understand E-safety issues through parents’ evenings, letters, text messages, emails, the school website and Dojo. Parents and carers will be responsible for:

- Endorsing (by signature) the Student/Pupil Acceptable Use Policy.
- Accessing the school computing systems or learning platforms in accordance with the school Acceptable Use Policy.

E-Safety in the curriculum

The school's delivery of the e-safety curriculum is closely linked to the PSHE curriculum and RSE and Health Education as well as being a significant part of the computing curriculum. Our delivery also takes into account the Prevent Duty and Keeping Children Safe in Education 2024; which categorises e-safety into four areas of risk:

•**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.

The curriculum through Common Sense Education ensures that children are taught the appropriate knowledge and safeguards to make sure they are not at risk of the content in the four Cs and in line with Teaching Online Safety in Schools document. This is also done in line with school and trust safeguarding policies. Our E-Safety curriculum is taught to the children from Y1 to Y6. Additional contextualised support is provided for children with SEND and vulnerable children e.g. those that have suffered from abuse in the past.

Units of the Common Sense Education curriculum include:

- Media Balance is Important
- Safety in my Online Neighbourhood
- Pause for People
- Pause and Think Online
- Internet Traffic Light
- How Technology Makes you Feel
- We, the Digital Citizens
- That's Private!
- Who is in your Online Community?
- Device-Free Moments
- Digital Trails
- Putting a Stop to Online Meanness
- Let's Give Credit!
- Your Rings of Responsibility
- This is me
- Password Power up
- Our Digital Citizenship Pledge
- The Power of Words

- Is Seeing Believing?
- My Media Choices
- Our Online Tracks
- Be a Super Digital Citizen
- Private and Personal Information
- Keeping Games Fun and Friendly
- A Creator's Rights and Responsibilities
- Finding my Media Balance
- Beyond Gender Stereotypes
- Is it Cyberbullying?
- You Won't Believe This!
- Digital Friendships
- Reading News Online

Remote Education

Owston Park adheres to COVID19 DfE guidance issued in March 2020 and follows guidance from Secure Schools on how to safeguard children in an online environment and follow the principles set out in the Guidance for Safer Working Practice for Those Working with Children and Young People in Education Settings published by the Safer Recruitment Consortium.

Owston Park ensures any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements. We report concerns immediately to Trust Central Office. All staff have had training on how to prepare children for, and manage, online behaviour and safety and also how they can protect themselves. All staff have undertaken training with regards to setting up secure live lessons, recordings and follow up activities.

E-safety teaching is continued and promoted during remote education due to children spending more time online. Our E-Safety curriculum is set as part of the remote education provision.

Children and parents are made aware of the online behaviour policy and expectations during live lessons to ensure safety for all parties concerned.

School devices are loaned to families following them signing an agreement to respect and use the devices for school related activities and education only.

Staff Training

All staff have safeguarding and Prevent training on a yearly basis, including online safety and all staff are made aware of relevant policies and procedures during their induction.

All staff are aware that technology is a significant component in many safeguarding and wellbeing issues. They are aware, through training and regular updates, that abuse can take place wholly online, or technology may be used to facilitate offline abuse and that in many cases abuse will take place concurrently via online channels and in daily life.

Staff know the correct procedures to follow if there is an online safeguarding concern.

Radicalisation, extremism, bullying and peer on peer abuse

- All of the above can be wholly online or facilitated by online elements.
- All staff are made aware of the indicators of cyber bullying, sexual exploitation, radicalisation and extremism, peer on peer abuse and all concerns are reported immediately to the DSL in line with safeguarding policies and the Prevent Duty.
- Cyber bullying can be defined as ‘Any form of bullying which takes place online or through smartphones and tablets.’ – BullyingUK.
- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school’s Child Protection Procedures**.** Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our Anti-Bullying Procedures. Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school’s policy on Anti-Bullying and Behaviour. Sexting between pupils will be managed through the Anti-Bullying Procedures.
- Extremism is defined by the Crown Prosecution Service as ‘The demonstration of unacceptable behaviour by using any means or medium to express views which:
  • Encourage, justify or glorify terrorist violence in furtherance of beliefs;

  • Seek to provoke others to terrorist acts;

  • Encourage other serious criminal activity or seek to provoke others to serious criminal acts;

  • Foster hatred which might lead to inter-community violence in the UK.
- The school understands that pupils may become susceptible to radicalisation through online sources as well as a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals. It is vital that school staff can recognise those vulnerabilities.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include;
• unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded;

• denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,

• making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.
If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.
Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as online bullying or general online safety.

System Security Management, Filtering and Monitoring

We take security very seriously at Owston Park.
As such:

- Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's computing systems. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.
- The computing technician from Wavenet will be responsible for regularly updating anti-virus software.
- School system security will be regularly reviewed. If additional security needs putting in place this will be discussed with our consultant from Wavenet alongside the Trust.
- Use of the equipment for computing will be in line with the school's policies and procedures.
- Pupils and parents will be aware of the school rules for responsible use of computing equipment and the internet and will understand the consequence of any misuse.
- Access to inappropriate websites is blocked. This will be checked and updated regularly to ensure the children do not have access to inappropriate content. Though

these safety measures will not affect teaching and delivery of the curriculum.

- If staff or pupils discover an unsuitable site, it must be reported to the DSL or Online Safety Lead immediately as well as Wavenet to ensure it cannot be accessed again. If inappropriate content is discovered DO NOT shut down the device but just close the lid so information can be gathered and the URL blocked.
- All staff and visitors need to read and sign the acceptable use policy before using school devices or internet.
- All information will be recorded, processed, transferred and used in accordance with GDPR Guidelines and the Data Protection Act.

The Rose Learning Trust

TRANSFORMING FUTURES COLLABORATIVELY