E-Safety Policy

Oakfield North Short Stay School – Shepshed

and

Oakfield South Short Stay School – Earl Shilton

Reviewed September 2024

E-Safety Policy

This E-Safety policy recognises our commitment to E-safety and acknowledges its part in the school's overall safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep pupils safe in the ever-increasing digital world and outlines the steps we take to ensure this happens. As part of our commitment to E-Safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets.

Responsibilities of the School Community

We believe that E-Safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The Management Team accepts the following responsibilities:

- Ensure adequate technical support is in place to maintain a secure IT system
- Ensure policies and procedures are in place to support the integrity of the school's information and data assets
- Ensure effective liaison with the Management Committee
- Make appropriate resources, training and support available to all members of the provision community to ensure they are able to carry out their roles effectively with regard to E-Safety
- Receive and regularly review E-Safety incident logs via CPOMS; ensure that the correct procedures are followed should an E-Safety incident occur in school and review incidents to see if further action is required
- Take ultimate responsibility for the E-Safety of the school community

Responsibilities of all Staff

- Read, understand and help promote the school's E-Safety policies and guidance
- Take responsibility for ensuring the safety of sensitive data and information
- Develop and maintain an awareness of current E-Safety issues and legislation and guidance relevant to their work
- Always maintain a professional level of conduct in their personal use of technology
- Embed E-Safety messages in learning activities and indirect teaching opportunities where appropriate

- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all E-Safety incidents which occur in the appropriate log (CPOMS) and/or to their DSL/SLT
- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Will not use personal mobile phones or electronic devices during work hours, unless on break or lunch
- Staff will only use school devices when contacting parents or pupils, recording or storing data, photos or information about pupils and families.
- Understand data protection laws around pupil and family data
- Staff must report an incident of E-safety or data breach as soon as possible or within the working school day (refer to GDPR policy)

Additional Responsibilities of Technical Staff

- Support provision in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school IT system, sensitive data and information. Review these regularly to ensure they are up to date
- At the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the AUP is being followed
- Report any E-Safety related issues that come to their attention to the E-Safety coordinator and/or leadership team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems
- Ensure that suitable access arrangements are in place for any external users of the school's IT equipment
- Liaise with the Local Authority and others on e-safety issues

Responsibilities of Parents and Carers

- Help and support the school in promoting E-Safety
- Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our community lies in effective education.

We know that the Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We believe that learning about E-Safety should be embedded across the curriculum and also taught in specific lessons in IT and PSHE.

We will discuss, remind or raise relevant E-Safety messages with pupils routinely wherever suitable opportunities arise.

Managing and safeguarding IT Systems

Oakfield Short Stay School North and South will ensure that access to the school IT system is as safe and secure as reasonably possible namely by ensuring that:

- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for activity.
- Any administrator/master passwords for school IT systems are kept secure and available to at least two members of staff
- The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by named individuals
- We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on provided laptops.

Using the Internet

We provide the internet to:

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA
- Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the IT systems or a provided laptop or device and that such activity can be monitored and checked.

- All users of the IT or electronic equipment will abide by the E-Safety Policy at all times, whether working in a supervised activity or working independently,
- Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the filename or in accompanying text online.

We ask all parents to sign an agreement about taking and publishing photographs and video of their children and this list is checked whenever an activity is being photographed or filmed.

For their own protection staff never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

Protecting data and information

Oakfield Short stay School North and South operate within the GDPR Regulations. We recognise our obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

Pupils are taught about the need to protect their own personal data as part of their E-Safety awareness and the risks resulting from giving this away to third parties.

Dealing with E-Safety incidents

All E-Safety incidents are recorded on CPOMS which is reviewed daily.

Instances of cyber bullying will be taken very seriously by the service and dealt with using the anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Incidents which create a risk to the security of the network, or create an information security risk, will be referred to the school's SLT and technical support. Appropriate advice will be sought, and action taken to minimize the risk and prevent further instances

occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy, then appropriate sanctions will be applied. The unit will decide if parents need to be informed if there is a risk that pupil data has been lost.

All incidents will be recorded on CPOMs.