ORION

E-SAFETY

POLICY

This policy will be kept up to date and will be reviewed once per year as part of the company's Quality Assurance arrangements.

Review Period	Approved by	Review Carried Out By	Date of Approval
1 Year	Directors/Governors	Quality Team	November 2020

On-line safety Policy

Introduction

Orion believes that the use of information and communication technology in education brings great benefits. This policy aims to recognise on-line safety issues and will help to ensure the appropriate, effective and safer use of electronic communications for all students and staff. We are aware that in today's society children, young people and adults interact with technologies such as; mobile devices (including phones, tablets, wearable technology e.g. smart watches), games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved can be greatly beneficial to all, but can also place people in danger. This on-line safety policy covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communication technologies, both in and out of the educational setting.

Aims

- To safeguard children, young people and staff.
- To be able to identify the risks associated with social networking.
- To identify roles and responsibilities and recognise that on-line safety is part of the 'duty of care' which applies to everyone working with children and young people.
- To educate and empower our students so that they possess the necessary skills to make safe and responsible decisions and to feel confident to report any concerns they may have.
- To raise awareness of the importance of on-line safety amongst all staff so they are able to educate and protect students in their care.
- To inform staff how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.
- To provide opportunities for parents/carers to develop their knowledge of on-line safety.
- To ensure awareness amongst all members of Orion that 'online actions can have offline consequences'.
- Orion identifies that the issues identified with on-line safety are considerable, but can be broadly categorised into 3 categories of risk including: Content (exposed to harmful materials), Contact (subjected to harmful online interactions) and Conduct (personal online behaviour that can result in harm).

Orion will ensure that:

- The on-line safety policy will be reviewed annually.
- Management team has responsibility for on-line safety.
- The School appoints a member of the Governing Body to take lead responsibility for on-line safety.
- A member of staff will be accredited with CEOP (Child Exploitation and Online Protection) training.
- All members of Orion's community will be informed about the procedure for reporting on-line safety concerns (such as breaches of filtering, Cyberbullying, illegal content).

- The Designated Safeguarding Lead will be informed of any on-line safety incidents involving Safeguarding concerns, which will then be acted on appropriately.
- Orion will manage on-line safety incidents in accordance with the School's behaviour and Anti-Bullying policies where appropriate.
- Orion will inform parents/carers of any incidents of concern as and when required.
- Where there is a cause for concern or fear that illegal activity has taken or is taking place, then Orion will contact the Children's Safeguarding Team for advice and/or escalate the concern to the Police.
- The Police will be contacted if a criminal offence is suspected.
- Any complaint about staff misuse must be directly reported to the Head of School.
- Orion will work in partnership with Parents/Carers and students to resolve issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and Safeguarding procedures.
- All members of Orion's community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any others.

Cyberbullying

Cyberbullying can be defined as 'The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone' DCSF 2007.

Many children, young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively and we have a duty to safeguard all students and staff.

When children or young people are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone. This can be harmful, threatening and a great source of anxiety. Where bullying outside the educational setting (such as online or via text message/voicemail) is reported to Orion, it will be investigated and acted on.

Orion will ensure that:

- Cyberbullying (along with all other forms of bullying) of any member of Orion will NOT be tolerated.
- There are clear procedures in place to support anyone affected by Cyberbullying.
- There are clear procedures in place to investigate incidents or allegations of Cyberbullying (see Anti-Bullying Policy).

Mobile Phones

Orion is a NO MOBILE PHONE SITE for students whilst in training. This also includes any other mobile or electronic devices such as tablets, smart watches and digital cameras.

This is because:

- Mobile phones, or any other mobile devices with integrated cameras could lead to Safeguarding/Child Protection, bullying and data protection issues with regard to inappropriate capture or distribution of images of students or staff.
- Mobile phone use can render students or staff subject to Cyberbullying.
- Internet access on mobile devices using cellular data cannot be filtered by the school.
- They can undermine classroom discipline.

Roles and Responsibilities

The overall responsibility of maintaining safeguarding and child protection including on-line safety remains with the designated safeguarding lead.

The Leadership and Management at Orion will ensure on-line safety is viewed as safeguarding issue and that practice falls in line with national and local recommendations and requirements including providing an up-to-date policy on staff code of conduct and behaviour policy. Management will also ensure suitable filtering and monitoring systems are installed and operational. Orion's curriculum will also have imbedded, on-line safety allowing students to develop their knowledge and awareness of on-line safety issues. Orion will also undertake risk assessment regarding the safe use of technology and use the assessment as one means of auditing and evaluating on-line safety practice strengths and areas of improvement.

Parents and Carers

Orion will encourage all parents/carers to read on line safety information and promote and reinforce safe on-line behaviours at home to their child. If a parent/carer identifies signs or behaviour that could indicate their child is at risk, they will be required to report it to the designated safeguarding lead.

Students and Staff MUST:

- Immediately report to a designated member of staff if they receive offensive or abusive emails, text messages or posts on social networking sites.
- Immediately report to a designated member of staff if they have information that another person has experienced any of the above.
- Not reveal personal details of themselves or others which may identify them and/ or their location.
- Set passwords to their accounts in and out of work.
- Deny access to unknown individuals and block unwanted communications on social network sites.
- Not publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Training and Engagement with Staff

Orion will ensure all staff members are aware of the on-line safety policy during their induction and are kept up-to-date with appropriate on-line safety training annually as-well as being able to contribute to shaping the policy itself.

See appendix regarding staff conduct on-line on social media outside of school.

Orion will ensure that technology including the internet used by Staff to deliver lessons complies with this policy.

Password Policy

All Orion staff members will have access the "L" drive Management system which is protected by password. Staff members are responsible for keeping their passwords secure. We recommend using strong passwords containing upper and lower case, numbers, letters and symbols and that passwords are changed very academic year or when there has been a compromise to security.

Accessing e-mails

Accessing e-mail will take place in accordance with data protection and confidentiality policies. The forwarding of any chain messages is not permitted and spam or junk mail will be locked and reported to the internet provider. Email's containing sensitive information will be sent using encryption for added security.

Staff Use of Personal Devices and Mobile Phones

Orion advises staff to keep mobile phones and devices in a safe and secure place and that they are either switched-off or put on silent during lesson times. Options such as Bluetooth or airtime and hotspot must be disabled during school time. Devices cannot be used during lesson times unless written permission by the Head of School has been given, likely due to emergency situations.

Personal phones cannot be used to contact parents/carers or students and pre-existing relations between a staff member and a parent/carer or student will be discussed with the Head of School.

Work-provided equipment such as tablets can only be used to take photographic evidence of students undertaking practical tasks in the workshop and personal phones cannot be used for this task. If this policy has been breached, action will be taken in-line with the Code of Conduct Policy.

Visitors Use of Personal Devices and Mobile Phones

Visitor and Parents/Carers must abide by Orion's policies when using personal devices and mobile phones. Orion will ensure appropriate signage and guidance is displayed across the building accessible to all visitors, parents/carers.

If a staff member has concerns regarding breach of policy, the Head of School will be informed immediately.

Work-provided Phones

Specific staff members will be issued with a work-phone and email address which is used to contact parents/carers and will be secured by a password and pin.

Responding to On-line Concerns

Orion will ensure staff members are aware of the process involved in reporting any on-line safety concerns including sexting (youth produced imagery), cyber-bullying and illegal contents.

All staff members must understand and adhere to confidentiality and follow official procedures when reporting concerns.

Where there is suspicion that illegal activity has taken place we will contact MASH, 999 or 101, if there is immediate danger or risk of harm.

Social Media for Recruitment and Selection

Orion will only view relevant social media websites as part of the pre-employment process, i.e. those aimed specifically at the professional market and used for networking and career development, such as LinkedIn.

Consequences of Failure to Comply with Legislation or Policies

If a user fails to comply with the provisions outlined in this document, their access to IT Systems may be withdrawn and future access may be restricted. This may impact on the individual's ability to undertake the duties of their job or continue their studies.

Serious or consistent non-compliance with this policy may be considered to be a disciplinary offence and will be dealt with in accordance with the company's disciplinary procedures or other appropriate action may be considered.

Acts of a criminal nature; or any safeguarding concerns may be referred to the police, Birmingham Safeguarding Children Board (BSCB) and other relevant agencies.

Monitoring and Reviewing

Orion will revise this policy following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure. Internet use and the evaluation of on-line safety mechanisms will be thoroughly monitored to determine this policy is applied consistently throughout. The Head of School will be informed of any concerns relating to on-line safety immediately and as appropriate. The Governing Body will nominate a Governor who will oversee on-line safety practices at Orion and report back to the Body of any incidents and issues including outcomes.

Appendix A

Staff Guidance for Participating in Social Networking

Whilst the usefulness of social networks (including, but not exclusive to, Facebook, Twitter, MySpace, YouTube, etc) is not disputed, Orion staff choosing to use them must do all they can to protect their reputations and the reputation of the School.

Protect Yourself

To ensure that all staff protect their reputations and their privacy you must:

- Not befriend students on social networking sites.
- Not access social network sites during working hours.
- Not post information or personal views about Orion, its staff, students or parents.
- Think carefully how you present yourself when posting images, joining a group or 'liking' pages as these choices say something about you.
- Choose your friends carefully, not accepting friend requests from students or parents.
- Control who can see your information (for example, setting 'friends only' on Facebook and 'protecting my tweets' on Twitter).
- Be careful about comments you post on friends' walls because, if their profiles are not set to private, your comments will be visible to everyone.
- 'Untag' yourself from any inappropriate content posted by others, or ask the person who has posted the content to remove it.
- Keep passwords secret.
- Report any incident to the appropriate member of staff in a timely manner.
- Do not leave a computer or any other device logged in when you are away from your desk unless you have 'locked' it.
- Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure that they are kept up to date.
- Use your school email address for work and personal email address for your private life; do not mix the two. This includes file sharing sites, for example Dropbox and YouTube. Remember that anything you post online is potentially public and permanent.

Prohibited Use

Users must not use social media in either work or personal time to:

- Make statements that could be deemed to be defamatory, offensive, obscene, abusive, proprietary, or libellous
- Make statements that would contravene this, or any other School policy.
- Discuss students or colleagues or publicly criticise Orion polices or personnel
- Post images or videos that include students on social networking sites
- List their School's e-mail address ''@Oriontraininganddevelopment.co.uk' as a contact address for personal social network accounts, other than those aimed specifically at the professional market and used for networking and career development, such as LinkedIn

- Misrepresent the School's interests, whether these interests are in the public domain or not.
- Act, without permission, as a spokesperson for the School.
- Carry out any action which adversely affects the School's reputation or undermines its core business or related interests.
- Publish information that would be in breach of the Data Protection or Information Security polices
- Staff and students should not create pages, sections, news groups or equivalent on social networking services that claim to be linked to or represent the School without authorisation from the Head of School.
- Misappropriate or infringe the intellectual property of other organisations and individuals.

General Rule

Social networks and their associated terminology ('wall', 'tag', etc) are constantly changing and situations may arise which this guidance does not cover. Therefore, a general rule to follow is to avoid compromising your professional position by always presenting yourself online to colleagues, students, parents and members of the community in the same way you would present yourself in person.

Taking Down Offensive Content

If online content is offensive or inappropriate, and the person or people responsible are known, you need to ensure that they understand why the material is unacceptable or offensive and request they remove it. Most social networks have reporting mechanisms in place to report content which breaches their terms. If the person responsible has not been identified, or does not respond to requests to take down the material, the staff member should use the tools on the social networking site directly to make a report. Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly. Before you contact a service provider, it is important to be clear about where the content is; for example by taking a screen shot of the material that includes the web address. If you are requesting that they take down material that is not illegal, be clear to point out how it breaks the site's terms and conditions. Where material is suspected of being illegal, you should contact the police directly.