John Port Spencer Academy

E-SAFETY POLICY

Safeguarding Team

Lead Designated Safeguarding Lead: Mr L Shepherd

Deputy Designated Safeguarding Lead: Mrs C Golaub

Designated Lead for Mental Health: Mr W. Perry

Designated Lead for Prevent: Mr N Collier

Designated Teacher for Looked After Children: Mrs K Thomas

Designated Lead for Sixth Form: Mrs G Barnett

Safeguarding Officer: Miss Southall

Acting Safeguarding Officer: Mrs M Pemberton

Designated Link Governor for Safeguarding: Emma Twigg

Other documents/policies referred to are:

John Port Spencer Academy's Child Protection and Safeguarding policy

John Port Spencer Academy's Sexting policy

Published: V2 – UPDATED
Revised: August 2018
To be reviewed: December 2018 or before

E Safety Policy

Strategy
This policy supports and is supported by the Academy policies on 'Child Protection and Safeguarding' and 'Sexting' as well as the 'Authorised User Policy for Students' (see Appendix 1).

Introduction
Digital and electronic devices offer dynamic and exciting services for both personal use and educational reasons. It is essential that schools and Academies provide a safe environment for children, young people and adults whether they are using printed or electronic resources.

This strategy has been designed to give an overview of how e-safety is managed and maintained within John Port Spencer Academy.

Background
E-Safety is principally recognised in relation to use of the internet. However, use of mobile devices also raises the need for awareness of e-safety principles.

The internet provides access to a wealth of information, educational and cultural content, as well as sites for general entertainment and for purchasing goods. However, the internet also provides content, which parents, carers and education professionals may not wish children to access. It is also possible for anyone to access content that may be deemed unacceptable for viewing in public areas, whether deliberately or not. All users need to be aware of the dangers of accessing unsafe sites and of the dangers of receiving inaccurate information through websites.

John Port Spencer Academy filters internet access on all computers using filtering software. This is designed to increase the level of internet safety. However, this cannot be totally secure and does not remove the responsibility of parents, carers or legal guardians for their children's internet use or adult users for their personal use.

John Port Spencer Academy has an Acceptable Use Policy, which all users are required to accept before they can access the internet.

John Port Spencer Academy Safe Internet Policy
Children are often the most adventurous but also the most vulnerable when it comes to the use of new technologies. Furthermore, children's usage of the internet is comparatively high.

Despite this, the number of reports of abuse, or access to children by adults through misuse, remains small. There is consensus on e-safety, which makes it clear that limiting children's use of new technologies or banning their use for specific age groups is not a sensible option.

Risks
The main risks for use of communication technologies for individuals are:

Self-generated - putting themselves at risk online by:
- Posting sexually themed content of themselves or friends in sexually themed online discussions
- Disclosing excessive personal information about their real life through on-line profiles and blogs which allows targeting
- Sharing information on-line with individuals who are not personally known to them
- Pretending to be older than they are

Technical capability combined with lack of awareness and understanding of risk:
- Taking on the opportunities online communities bring not as an adjunct to their lives but as an integral part of it
- Having an advanced use of technology but not having a full understanding of risks and threats

Privacy and protection of personal data:
- Giving personal and financial information on mobile devices in public areas
- Having a lack of understanding of how data can be misused

- Being so used to giving personal data for registration on sites that it desensitises them to giving out personal information
- Sharing passwords
- Saving passwords on public machines

Cyberbullying:

- Bullying using mobile devices, either voice or text bullying and email bullying is on the increase – this is not just child on child but can often be child on adult
- Inappropriate use of photographs

PRINCIPLES & GUIDELINES FOR E-SAFETY

Digital and electronic communication in the Academy is not restricted to the Academy provided desktop, laptop or tablet computers. Members of the Academy also have access to their own mobile devices.

- E-safety in the Academy is a shared responsibility between the Academy, parents and students.
- The acceptance of an Authorised User Policy is an integral part of accepting responsibility.

6.1 Users are educated in safe use technology through:

- E-safety elements built into the delivery of ICT and Computer Studies lessons
- Regular awareness raising across the Academy via assemblies and leaflets.

6.2 Users are empowered to report abuse if it occurs through:

- Drawing attention to the CEOP (Child Exploitation and Online Protection Agency) reporting button, which is available on many websites.
- Being encouraged to report abuse to the Safeguarding team or to any adult in the Academy.
- Informing parents and young people about websites on e-safety via the Academy web pages and raising awareness regarding e-safety with parents and carers to ensure they can play a role in protecting their children and young people.

6.3 Abuse is minimised through:

- Managed filtering throughout the service
- Advising users of mobile devices of the safety issues due to lack of filtering on the public wireless service.

6.4 Staff are empowered to assist users to use the computer safely and to report abuse through:

- E-safety training for all frontline staff, to raise awareness of e-safety and how it relates to safeguarding children
- Ensuring staff are aware of internet sites that give advice including the Internet Watch Foundation and Child Exploitation Online Protection (CEOP)
- Ensuring staff are aware of the reporting systems in place.

6.5 Staff are fully aware and briefed on e-safety through:

- Training to make staff aware of the 'Acceptable Use Policy for staff' and their responsibility for their own internet use to ensure they do not misuse the computers.

'E-SAFETY' POLICY - APPENDIX 1

Acceptable Use Policy for Students

John Port Spencer Academy - Guidelines for Students (AUP)

This Academy has provided computers for the benefit of all students and staff, offering access to software, email and the Internet. You are encouraged to use and enjoy these resources to help you in your studies.

You are responsible for good behaviour when using the computers and the Internet just as you are in a classroom or on Academy premises.

These guidelines clearly state what is acceptable and what is not.

Remember that accessing the Academy network is a privilege, not a right and inappropriate use will result in that privilege being withdrawn and disciplinary action taken.

- Always make sure you have received permission to use a computer from a member of staff.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.
- You must respect the equipment at all times. Damaging, disabling or incorrectly adjusting the computer equipment in any way will not be tolerated.
- Always log off your station when you have finished working and leave your work area tidy.
- Keep your log on ID and password to yourself. You must never log on to the Academy network under someone else's log on name and password.
- You should be aware that your files and communications could be viewed by the network manager to ensure the system is being used responsibly.
- You should only use the computers and access the Internet for educational purposes and/or authorised/supervised activities. Do not waste your time and the resources.
- You may use e-mail with permission from a member of staff but you must not transmit material that is illegal and dangerous or offensive in any way.
- You should only open e-mails if they come from somebody you already know and trust.
- You should not use the Academy network for "chat" activities. You are taking up valuable resources that could be used by others.
- You may download text and images from the internet to help you with your work. You must respect copyright and not pass work off as your own; this is plagiarism and is forbidden.
- You must not use the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials that are illegal and dangerous or offensive in any way.
- When using the internet you should not reveal your home address and telephone number nor your Academy's name and contact details.
- You must not attempt to download or install programs on to the Academy network. Playing games and downloading music is forbidden.

Failing to comply with these guidelines will lead to loss of access to the Academy network and Internet. Additional action may be taken by the Academy in line with existing policies regarding Academy behaviour.

For serious violations, suspension or expulsion may be imposed. If appropriate, the police may be involved or other legal action taken.