E-SAFETY POLICY

Safeguarding Team

Please see the safeguarding page on our website for the latest information about our Safeguarding Staff Team

This policy should be read alongside:

Working together to safeguard children July 2018
Keeping children safe in education 2021
John Port Spencer Academy (SAT) Child Protection and Safeguarding Policy
John Port Spencer Academy (SAT) Peer on Peer Abuse Policy
John Port Spencer Academy Behaviour Policy
John Port Spencer Academy Anti-Radicalisation Policy

Included in this policy

Published: September 2020
Updated: November 2021
To be reviewed: December 2022 (or before)

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

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. The internet does, however, also provide 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 (see Appendix 1), which all users are required to accept before they can access the academy internet. We also have an Acceptable Use Policy specifically for guidance when teaching remote live lessons (see Appendix 2).

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 and 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.

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.
- Enrichment Days

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.

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.

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.

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.

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 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.

APPENDIX 2 - Acceptable Use Policy for Remote Learning: Live Lesson Expectations

Remote live lessons will be used in the event of a whole class being absent. Remote live lessons may be used in the case of part of a class being absent.

Links to: Safeguarding Policy; Data Protection Policy; Behaviour Policy, Acceptable Use Policy.

The following expectations relate to remote live lessons.

Leadership Oversight and Approval

1. Remote live lessons will only take place using Google Meet.
2. Staff will only use John Port Spencer Academy managed accounts with learners (and parents/carers).
3. Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
4. Any pre-existing relationships or situations which mean this cannot be complied with must be discussed with the Designated Safeguarding Lead.
5. Staff will use work provided equipment where possible e.g. a school laptop, tablet or other mobile device. If this is not provided, and staff are using their own devices, it is the member of staffs' responsibility to ensure the schools expectations are adhered to in relation to safeguarding and data security. This includes:
    - using strong passwords,
    - suitable levels of encryption,
    - using own log in (not sharing others log ins e.g. Google Account),
    - logging off or locking devices when not in use etc.
6. Remote live lessons will usually take place within timetabled lesson times during the school day. If there needs to be an exception to this, it will be checked with the senior leadership team. A member of the senior team, the designated safeguarding lead and/or head of department is able to drop in at any time.

Data Protection and Security

7. Only members of John Port Spencer Academy will be given access to Google Meet
8. Access to Google Meet will be managed in line with current IT security expectations.
9. All remote live lessons will take place in line with current John Port Spencer Academy confidentiality expectations as outlined in the SAT Data Protection Policy.
10. All participants will be made aware that Google Meet records activity. The teacher will inform the participants when the recording begins and ends.
11. Consent from those involved in the session is required if live lessons are recording activity. Recordings will be stored on the Teacher's Google Drive and uploaded to Google Classroom if required. Recordings will be kept only for the length of time they are useful e.g. for revision or recap. Recordings should not be shared with people outside John Port Spencer Academy.
12. All participants will be made aware that the recordings will be uploaded to Google Classroom, accessed by the class members and other teachers.

Session Management

13. Staff will keep a record of any remote live lessons held.
14. When conducting remote live lessons, appropriate privacy and safety settings will be used to manage access and interactions. This includes keeping meeting IDs private; only use Google Meet, using the academy Google account.

15. Contact will be made via learners' John Port provided email accounts and/or logins.
16. Staff will mute/disable learners' cameras and microphones if necessary.
17. Students will be instructed to turn off camera before recording begins and staff only start recording when this has taken place.
18. Staff will ensure all learners have left the session before they themselves leave
19. Live 1 to 1 sessions will only take place with approval from the Principal or member of the senior leadership team.
20. Invitations to remote live lessons should be via Google Classroom stream or school email
21. Access links should not be made public or shared to others outside the class except to line managers or senior staff when requested.
22. Learners are encouraged to attend remote live lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
23. Class members who do not access the remote live lessons should be raised with the Head of Faculty/Department to identify any concerns. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour Expectations

24. Staff will model safe practice and moderate behaviour online during remote live sessions as they would in the classroom.
25. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session. All participants are expected to behave in line with existing John Port Spencer Academy policies and expectations.
26. Staff will not take or record images for their own personal use.
27. When using remote live lessons, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
28. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

29. Participants are encouraged to report concerns during remote live lessons sessions. Concerns should be reported to either the teacher running the session, a parent/carer, another teacher or the safeguarding team.
30. If inappropriate language or behaviour takes place, participants involved could be removed by staff, the session may be terminated, and concerns will be reported to the Head of Faculty /Department.
31. Inappropriate online behaviour will be responded to in line with John Port Spencer Academy existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
32. Sanctions for deliberate misuse may include:
    - restricting/removing use
    - exclusion from online lessons
    - contacting the police if a criminal offence has been committed.
33. Any safeguarding concerns will be reported to the Designated Safeguarding Lead, in line with our child protection policy.