Yeoman Park Academy

Online Safety Policy Appendix September 2020

Office use

Published;	**Next review:**	**Statutory/non:**	**Lead:**
September 2020	September 2021	Statutory	Shona Doyle

DAT Online Safety Policy https://www.diverseacademies.org.uk/wp-content/uploads/sites/25/2020/12/Online-Safety.pdf

Associated documents:

YPA Anti-Bullying Policy
YPA Safeguarding & Child Protection Policy
YPA Safeguarding & Child Protection Policy Covid Appendix

Links to:

DAT Anti-Bullying Policy
https://www.diverseacademies.org.uk/wp-content/uploads/sites/25/2019/08/Anti-bullying.pdf
DAT Safeguarding & Child Protection Policy

https://www.diverseacademies.org.uk/wp-content/uploads/sites/25/2018/10/Safeguarding-and-Child-Protection.pdf

Introduction

This document is based upon the principles based in the Diverse Academies Online Safety Policy: https://www.diverseacademies.org.uk/wp-content/uploads/sites/25/2020/12/Online-Safety.pdf

Yeoman Park is committed to supporting all members of the academy community to understand both the benefits and the risks of technology, and to equip pupils with the knowledge and skills to be able to use technology safely and responsibly.

Writing the online safety policy

- The Online Safety Policy relates to other policies including those for ICT, anti-bullying and for child protection.
- The **Designated Safeguarding Lead** is Sharon Savage
- The academy's **Online Safety Coordinator** is **Shona Doyle**.
- The **governor** responsible for online safety is **Pete Edwards**
- Our online safety Policy has been written by the academy with regard to the DAT and DfE guidance.
- This policy applies to all members of the academy community including staff, parents/carers, students/pupils, volunteers, and community users, who have access to and are users of school ICT systems, both in and out of school.

What is online?

- Online safety is "About the issues associated with information systems and electronic communications as a whole." This includes not only the internet but all electronic communications such as; mobile phones, games consoles, cameras, and webcams. We need to be aware of the increasing access to digital technology through the range of mobile devices.
- Issues relating to e-safety need to be seen as part of the Safeguarding children agenda, not just ICT.
- It is the responsibility of all, to understand the risks, acceptable use, as well as how to respond to incidents involving online safety, both in and out of the academy environment.

Internet Use for Children and Young People with SEN

Children with SEN are potentially more vulnerable and more at risk than others when using ICT:

- Those children with ASD may make literal interpretations of content which will affect how they respond.

  They may not understand some of the terminology used.
- Those with more complex needs do not always understand the concept of friendship and therefore trust everyone implicitly. They do not know how to make judgements about what information is safe to share. This leads to confusion about why you should not trust others on the internet.

- Some children may be vulnerable to being bullied through the internet and may not recognize that they are being bullied.
- They may not appreciate how their own online behaviour may be seen by someone else as bullying.

Aims of the online safety policy are to ensure that:

- We protect and educate pupils and staff in their use of technology
- Teachers and parents understand that they have a part to play in safeguarding the protection of pupils at school and at home respectively
- Pupils, staff, and parents are educated to understand about cyber-bullying, including the likely consequences
- Policies and procedures are in place to help prevent incidents of cyber-bullying within the school community
- We have effective measures to deal with and monitor cases of cyber-bullying

Teaching and learning

The Internet is an essential element in 21st century life for education, business, and social interaction. The academy has a duty to provide students with quality Internet access as part of their learning experience in order to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the academy's management functions.

It is also part of the statutory curriculum and a necessary tool for staff and pupils. Yeoman Park Academy ensures that:

- The academy internet access is designed expressly for pupil use and includes filtering appropriate to the needs of our pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet.
- Parents will be supported by:
    - Information on the safe use of the internet for their families where applicable
    - A link to useful resources on our academy website

Introducing the online safety policy to pupils

- Online safety rules, in a format appropriate for our pupils, will be posted in classrooms and discussed with pupils as part of their learning, where appropriate.

- Pupils will be informed that network and internet use is monitored.

Online safety and cyber-bullying training will be embedded within the ICT teaching and learning document and the Personal, Social and Health Education (PSHE) curriculum

Internet

Pupils are taught how to evaluate Internet content

- The academy ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught, where appropriate to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit
- Pupils will be taught how to report unpleasant internet content to their class teacher, parent, or carer
- Ensure all staff and pupils understand the importance of password security and the need to log out of accounts
- All staff must read and sign the 'Staff code of conduct' before using any academy ICT resources
- The academy will maintain a current record of all staff and pupils who are given access to IT systems.
- Any person not directly employed by the academy will be asked to sign an 'Acceptable use of school ICT resources' before being allowed to access the internet from the academy site. **(Appendix 1)**

Cyberbullying

Cyber-bullying will also be addressed in the anti-bullying policy along with other forms of bullying. Cyber-bullying should also be addressed in ICT, PHSE and other lessons when appropriate. The academy will proactively engage with pupils in preventing cyberbullying by:

- Understanding and talking about cyberbullying
- Keeping policies and practices up to date with new technologies Ensuring easy and comfortable procedures for reporting
- Complaints should be dealt with as with all bullying incidents following the procedures set out in the Anti-bullying policy
- Any complaint of staff misuse should be directed to the Principal

- Promoting the positive use of technology
- Evaluating the impact of prevention activities
- Records of any incidents of cyberbullying will be kept and will be used to help to monitor the effectiveness of the academy's prevention activities.

Information system security

- Academy ICT systems, capacity and security are reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with DAT

E-mail

- Pupils are not given their own e-mail accounts on the academy system, but where appropriate an approved email address for their use will be set up for curriculum purposes that is monitored at all times by the class staff.
- In an email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on headed paper.
- The official academy email service may be regarded as safe and secure and is monitored.
- Users must immediately report, to the nominated person, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond in any communication **Published content and the school web site**
- The contact details on the website are the academy address, e-mail, and telephone number. Staff or pupils' personal information will not be published. Careful monitoring will ensure that the site is GDPR compliant
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

Pupil's images and work

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Digital images may remain on the internet forever and may cause harm or embarrassment to individuals.

- Pupils' names will not be used anywhere on the website, particularly in association with photographs.
- Photographs that include children will be selected carefully.
- Written permission from parents or carers for the use of photographs on the website is requested as part of the annual data collection process.
- When using digital images, staff should inform and educate pupils, where appropriate about the risks associated with taking, sharing, publication and distribution of images.
- In accordance with guidance from the Information Commissioner's Office parents/carers are welcome to take videos/digital images of their children at school events for their personal use (as such use in not covered by the Data Protection Act & GDPR). To respect everyone's privacy and, in some cases, protection, these images should not be published or made publicly available on social networking sites.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individual or the academy into disrepute.

Social networking and personal publishing

Staff are made aware that their use of social networking applications has implications for our duty to safeguard children, young people, and vulnerable adults. Expectations for teacher's professional conduct are set out in 'Teacher's Standards 2012'. The academy has a duty of care to provide a safe learning environment for pupils and staff. The academy could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members, who harass, cyber-bully, discriminate on the grounds of sex, race, or disability or who defame a third party may render the academy or DAT liable to the injured party.

- Academy staff should ensure that no reference is made in social media to pupils, parents/carers, or academy staff

  Staff should not engage in online discussion on personal matters relating to members of the school community
- Staff should ensure that security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- Staff should ensure that any technological equipment is password/PIN protected
- The academy will block/filter access to social networking sites using the DAT filtering software.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

- Children/ young people and their parents/ carers **should not** be accepted as friends
- Pupils and parents will be advised that the use of social network spaces outside the academy brings a range of dangers for our pupils. **Managing filtering**
- The academy will work with DAT IT services to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Principal.
- The teachers will ensure that they make regular checks to ensure that the filtering methods selected are appropriate, effective, and reasonable. Any issues will be reported to the Principal.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the academy is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. **The use of mobile phones**
- Personal mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate messages is forbidden either by text, Bluetooth, or any other means
- If you are lone working with a pupil then you may keep your personal mobile phone with you, however, this must only be used to contact another member of staff if you need further support.
- Personal phones **MUST NOT** be used to take photographs of pupils.
- Staff will use an academy phone when contact with pupils and their families is required
- Each class has access to their own iPad and iPod which can be used to capture photographs of pupils on educational visits if required.

Games machines

- If games machines, including the Sony PlayStation, Microsoft X box, Nintendo Wii and others which have internet access, are used in the academy these must have a filtering system **Protecting personal data**
- Personal data will be recorded, processed, transferred, and made available according to the GDPR guidelines.

Assessing risks

- The academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on an academy computer. Neither

the academy nor DAT can accept liability for the material accessed, or any consequences of internet access.

- The academy will audit ICT provision to establish if the Online safety policy is adequate and that its implementation is effective.
- The academy will complete individual safety plan for those pupils considered to be at risk. **(Appendix 3)**

Handling online safety complaints

- Complaints of internet misuse will be dealt with by the Principal
- Complaints of a child protection nature must be dealt with in accordance with academy child protection procedures.

Staff and the online safety policy

- All staff will be made aware of the academy online safety policy and its importance explained.
- A copy of the policy will be available for all staff
- A copy of the DAT policy statement will also be available for all staff
- Staff will be made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

Enlisting parents' support

Parents' attention will be drawn to the academy e-Safety Policy in newsletters, and the academy Web site. Parent/Carers consent form and online safety rules letter will be sent to parents/carers where appropriate. **(Appendix 2)**

Academy Actions and Sanctions

It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal/disciplinary procedures as follows:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported
- Conduct the procedure using a designated computer that will not be used by young people, use the same computer for the duration of the process

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may be necessary to record and store screen shots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form (except for images of child sexual abuse-see below)
- Once this has been completed and fully investigated it will need to be decided whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

  - Internal response or discipline procedures
  - Involvement by DAT or national/local organisation (as relevant) - Police involvement and/or action

- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other incidents to report to the police would include:

  - Incidents of grooming
  - The sending of obscene materials to a child
  - Adult material which potentially breaches the Obscene Publications Act
  - Criminally racist material
  - Other criminal conduct, activity, or materials

- Isolate the computer as best you can. Any change to its state may hinder a later police investigation

Appendix 1

Staff, Governor and Visitor Template Acceptable Use Policy/ICT Code of Conduct Yeoman Park Academy

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our working life in the academy. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its content.

- I appreciate that ICT includes a wide range of systems and devices including mobile phones, PDA's, digital cameras, email, social networking and may include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use an academy ICT system for a purpose not permitted by its owner.
- I will comply with the ICT system security and not disclose any passwords provided to me by the academy or other related authorities.
- I understand that I am responsible for all activities carried out under my username.
- I will only use the academy email, internet, intranet, Learning platform or any related technologies for professional purposes.
- I will ensure that personal data is kept secure and used appropriately, whether in the academy, taken out of the academy or used remotely when authorised by the Principal or Governors
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal, or discriminatory.
- I will respect copyright and intellectual property rights.
- Images of pupils and/or staff will only be taken, stored, and used for professional purposes in line with academy policy and consent of the parent, carer, or staff member. Images will not be distributed outside the academy network/learning platform without permission.
- I will ensure that my online activity both in and outside the academy will not bring my professional role into disrepute.
- I will ensure that all electronic communications with parents, pupils and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the academy e-safety policy and help pupils to be safe.
- I will report any incidents of concern regarding children's safety to the e-safety co-ordinator, the Child Protection Officer, or the Principal.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the Police.

User Signature

I agree to follow the code of conduct and support the safe use of ICT throughout the academy.

Full Name: _____

Job Title: _____

Signature: _____ Date: _____

Appendix 2

Parent/Carers consent form and online safety rules

All pupils will have access to the academy's computer facilities including the internet as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the online safety rules have been understood and agreed.

Pupils Name: _____

Parent/Carers Name: _____

- As the parent or legal guardian of the above pupil, I have read and understood the attached academy rules and now grant permission for my son/daughter to use the internet, school e-mail system, learning platform and other ICT facilities at school.

- I know that my son/daughter has signed an e-safety agreement and they have a copy of the school online safety rules.

- We have discussed this document and they agree to follow the rules to support the safe and responsible use of ICT at the academy.

- I accept that the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that they will take every reasonable precaution to keep pupils safe and prevent pupils accessing inappropriate materials.

- The academy has an educationally filtered service, restricted access to email and provides age appropriate teaching around internet use and online safety issues.

- I will support the academy by promoting safe use of the internet and digital technology at home and will inform the academy if I have any concerns over my child's online safety.

Parent's/carer's Signature(s): _____ Date: _____

Appendix 3

Name: X **DOB:** 12.09.2004	**Date:** 31.10.XX
Summary of current knowledge and awareness of online safety	• X is competent at using ICT and the internet for researching his interest, for playing games and watching videos • X is aware that some people who use the internet are not nice and he knows the term 'cyberbully' and 'troll'. He said if he thought he was being bullied online he would tell his teacher • X does not like to use iPads or other Apple devices believing them not to be as good as Microsoft for gaming
What does pupil want / need to be able to access (Email / internet / social networking etc.)	• X likes to watch funny videos on YouTube. Most funny ones but also ones about paranormal activity • X does not use Twitter – he says you need to be 15 • X has an email account but has forgotten the password • X has a Facebook account but says he cannot access it at the moment. He says his account is private. He has a picture of Dennis the Menace so people cannot see his picture • X uses X Box live to play games and talks to people who he does not know – he says he would stop playing if they were unkind to him.
Potential Risks	• Online gaming and chatting to unknown people • Accessing content that may be too old for him and may scare and worry him (e.g. paranormal activity) • Accessing inappropriate videos by accident that may be named one thing but contain something different
Key Priorities	• X to enjoy his own free time • X to be able to play games in his bedroom safely • X to develop an understanding of how to keep safe online
Strategies / Control Measures	• Class / group teaching about safe use of the internet including demonstrations of how to keep safe when using social media • Work with parents to put control measures in place at home

Signed on behalf of Yeoman Park Academy ……..…….

Signed by pupil (if appropriate)…..…….

Date ……..…….