Drapers’ Academy

# Online Safety Policy - DCP 003

**Policy Owner:** Sue Monk **Policy Date:** September 2020

## Introduction

New technologies have become integral to the lives of children and young people, both within school and their lives outside.

The Drapers’ Multi-Academy Trust (MAT) supports this development but within a framework of use that helps pupils to be responsible, to use the technology and applications in an appropriate manner and to stay safe. This policy outlines how children and staff will be safeguarded and protected online.

## Scope

This policy applies to all staff and pupils of the Drapers’ Academy. It also applies to parents and carers of pupils at the school who formally confirm that they will abide by our policies when their children join our school.

The Academy must ensure that the contents of this policy are communicated to all staff. This communication must be evidenced as received in writing and refreshed on an annual basis. All parents must formally accept this policy when their children join the Academy and this acceptance must be evidenced in writing through the Home-School Agreement.

The Academy must publish this policy on its website.

## Definitions

| | |
|---|---|
| **Child** | Anyone under the age of 18 |
| **OSO** | Online Safety Officer |
| **DSL** | Designated Safeguarding Lead |
| **LGB** | Local Governing Body, with delegated powers of governance from the board of the MAT |
| **MAT** | Drapers’ Multi-Academy Trust |
| **Parent** | Those having parental responsibility for the care of a Child (including Carers) |
| **Pupil** | Anyone enrolled at Drapers’ Academy (including students in Years 12 and 13) |

**Social Media** Websites and phone apps designed for sharing information. These include, but are not limited to, blogs, online discussion forums, collaborative spaces, personal networking such as 'Facebook', media-sharing such as 'YouTube' and micro-blogging such as 'Twitter'

**Staff** Anyone employed at the Academy, including volunteers and governors ?

**Policy**

The main areas of risk, linked to online safety, for the community can be summarised as follows:

a. Content

i. Exposure to inappropriate content

ii. Lifestyle websites promoting harmful behaviours

iii. Hate content

iv. Content validation: how to check authenticity and accuracy of online content

b. Contact

i. Grooming (sexual exploitation, radicalization etc)

ii. Online bullying in all forms

iii. Social or commercial identity theft, including passwords

c. Conduct

i. Aggressive behaviours (bullying)

ii. Privacy issues, including disclosure of personal information

iii. Digital footprint and online reputation

iv. Health and well-being (amount of time spent online, gambling, body image)

v. Sexting

vi. Copyright (little care or consideration for intellectual property and ownership)

**Responsibilities of the Principal**

1. The Principal/DSL must be adequately trained on off-line and online safeguarding, in line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance

2. The Principal/DSL of the Academy is responsible for establishing procedures for ensuring Online Safety. These must be approved by the LGB

3. The Principal must appoint an Online Safety Officer (OSO) and determine what training they require and the level of attainment they must achieve

4. The Principal must ensure that an appropriate Online Safety programme is included in the curriculum, ensuring that online safety is fully integrated with whole school safeguarding e.g. PSHE/RE Curriculum

5. The Principal must ensure that parental permission is obtained before using images of any pupil in the school in publicity material or on the school website

6. The Principal has the authority to monitor the use of the Academy's information systems, including email accounts, and access to the Internet. They have the right to authorise the deletion of offensive material

**Responsibilities of the Online Safety Officer**

7. The OSO must:

    i. Be fully trained on Online Safety (in accordance with section 2 above) and provide guidance and training to the SLT and to staff

    ii. Ensure that their training is up to date

    iii. Take responsibility for the operation of Online Safety procedures and ensure that these are communicated to, and followed by, all staff (including online lessons, Zoom, Loom, FROG, DPR etc.)

    iv. Liaise with the shared services technical staff

    v. Carry out an annual audit of Online Safety training needs and address any deficiencies identified

    vi. Provide appropriate training to all those user groups set out in this policy so that they are able to discharge their responsibilities

    vii. Ensure that Online Safety training is included in the induction programme for all new staff (see iii)

    viii. Receive reports of all Online Safety incidents, record these and recommend any remedial action to the Principal, unless it is a safeguarding concern which should be reported directly to the Nominated Safeguarding Lead (through CPOMS)

    ix. In circumstances where there is a concern that a crime has been committed the OSO will, in conjunction with the Principal, contact the Police

**Responsibilities of the MAT Technical Staff**

8. The Principal must ensure that the Academy has access to the appropriate technical expertise to comply with the requirements of this policy

9. Technical staff must:

   i. Ensure the Academy's IT infrastructure is secure and is not open to abuse or malicious attack

   ii. Ensure that users can only access the Academy's networks through a properly enforced password protection or other control system

   iii. Operate a filtering process as determined by the Principal and update it as necessary

   iv. Put in place control mechanisms to prevent access to inappropriate websites

   v. Monitor usage of the system for potential E-Safety breaches

   vi. Remove offensive content

   vii. Report any breaches of this policy to the Principal/DSL

   viii. Keep up to date with E-Safety technical information and inform and update others as necessary

**Responsibilities of Staff**

10. Staff must:

   i. Sign an Acceptable Use of the Internet declaration at the start of employment

   Staff will be reminded of this declaration annually and a notice will be sent out via the staff bulletin

   ii. Have an up to date awareness of Online Safety matters, this policy and the supporting procedures

   iii. Report any suspected misuse or problem to the Principal/OSO/DSL

   iv. Only communicate with pupils on a professional basis and only use official school communication systems

   Follow the Drapers' Academy "Remote Online Learning Procedures" document

   v. Only take and use images of pupils for educational purposes and only use school equipment for such purposes (check parental permission is in place)

   vi. Ensure that E-Safety issues are embedded in all aspects of the curriculum and other school activities

   vii. Ensure that pupils understand and follow the school Online Safety Procedures

   viii. Ensure that pupils have an understanding appropriate to their age of research skills and the need to avoid plagiarism and uphold copyright regulations

   ix. Monitor ICT activity in lessons, extra-curricular and extended school activities

x. Be aware of Online Safety issues relating to the use of mobile phones, cameras and hand-held devices and that they monitor their use

xi. Guide pupils/students to websites that are suitable to their use and ensure that they are equipped to deal with any unsuitable material that is found in Internet searches

xii. Report any breaches of this policy to the Principal and the OSO

**Responsibility of Pupils**

11. Pupils must:

i. Sign an Acceptable Use of the Internet declaration

ii. Use the school IT systems in accordance with the Online Safety procedures

iii. Understand the importance of securing their passwords and not allowing others to log on using their ID

iv. Have an understanding appropriate to their age of research skills and the need to avoid plagiarism and uphold copyright regulations

v. Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do

vi. Understand the risks associated with publishing images of themselves on social media

vii. Not take, use, share, publish or distribute images of others without their permission

viii. Understand school procedures on the use of mobile phones, cameras and hand-held devices

ix. Understand that taking and using inappropriate images, and other forms of cyber-bullying are expressly prohibited and will be dealt with through the mechanisms set out in the Child Protection and Safeguarding Policy. This also applies to usage out of school hours

x. Understand the importance of adopting good Online Safety practice when using digital technology outside of school

**Staff Use of Email**

12. Staff emails are not confidential

13. Personal data (MAT Data Protection Policy) must not be transmitted by email unless adequate encryption facilities are used

14. Staff must not make defamatory comments or use inappropriate language, or otherwise communicate in an unprofessional manner

15. Staff must never use a false identity

16. Staff must not use their email to create or distribute offensive or unwanted email, including the dissemination of chain messages

17. Staff are responsible for all material they download from the Internet

**Social Networking Sites**

18. The use of social media within the Academy is only allowed in appropriately controlled situations and in support of legitimate curriculum activities

19. Staff and pupils must not access social media for personal use using school information systems, school networks or using school equipment

20. Outside of directed time, staff may access social media using their own personal computer, phones etc., but they should never give out personal information that is inappropriate to their position and responsibilities.

21. Staff must not post inappropriate photographs of themselves on social media and must not post photos of colleagues or any school related activity.

22. Staff must not post comments or views regarding the MAT or its schools on social media.

23. Staff are prohibited from communicating with pupils and parents of pupils using social media

**Prohibited Use of MAT Networks and IT Facilities**

24. The following are prohibited on the Academy networks and IT Facilities:

    i. Illegal activities

    ii. Accessing or downloading pornographic material

    iii. Gambling

    iv. Soliciting for personal gain or profit

    v. Managing or providing a business service other than one expressly approved by the Principal

    vi. Revealing or publicising proprietary or confidential information

    vii. Representing personal opinions as if they were those of the MAT or the school

    viii. Making or posting indecent or offensive remarks or proposals

**Sanctions**

25. Staff breaches of the requirements of this policy will be addressed through the MAT Disciplinary Policy

26. Pupil breaches of this policy will be addressed through the Pupil Disciplinary Sanctions Policy - DCP 018

**Review**

24. The policy owner must keep up to date with relevant legislation and government guidance and update this policy whenever necessary. The LGB must approve the revised version

25. The policy owner must review the policy at the end of July each year and either submit a revised policy for LGB approval and confirm in writing to the Principal that the current version of this policy is still fit for purpose

26. The Principal must submit a list of all confirmed policies to the board at the first meeting of each new academic year

27. The MAT board must formally review and re-approve this policy every five years