

**Online Safety Policy**

January 2024

Contents

[1 Introduction 3](#_Toc161217902)

[1.1 Purpose 3](#_Toc161217903)

[1.2 Scope 3](#_Toc161217904)

[1.3 Classification of online risks 3](#_Toc161217905)

[2 Roles and responsibilities 4](#_Toc161217906)

[2.1 Chief Executive Officer and Director of Operations 4](#_Toc161217907)

[2.2 Designated Safeguarding Lead 4](#_Toc161217908)

[2.3 All staff 4](#_Toc161217909)

[2.4 Students 5](#_Toc161217910)

[3 Student acceptable use statement 5](#_Toc161217911)

[3.1 Students’ own personal safety 5](#_Toc161217912)

[3.2 Respect for and the safety of others 5](#_Toc161217913)

[3.3 Responsible use of school and Dusemond IT 6](#_Toc161217914)

[4 Staff acceptable use statement 6](#_Toc161217915)

[4.1 Professional and personal safety 6](#_Toc161217916)

[4.2 Responsible use of school and Dusemond IT 6](#_Toc161217917)

[5 Responding to online safety incidents, concerns or disclosures 7](#_Toc161217918)

[5.1 Responding to online safety incidents involving students 7](#_Toc161217919)

[5.1.1 Responding to online abuse/child-on-child abuse disclosure 7](#_Toc161217920)

[5.1.2 Incident of student misuse 8](#_Toc161217921)

[5.1.2.1 Responding to nudes/semi-nudes incidents (sexting) 8](#_Toc161217922)

[5.1.2.2 Upskirting incident 9](#_Toc161217923)

[5.1.2.3 Cyberbullying incident 9](#_Toc161217924)

[5.2 Procedures for dealing with online safety incidents involving staff 9](#_Toc161217925)

[6 Social media 9](#_Toc161217926)

[6.1 Personal use of social media – staff 9](#_Toc161217927)

[6.2 Personal social media use – students 10](#_Toc161217928)

# 1 Introduction

Being online is an integral part of children’s lives. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form part of children’s online world. The internet and online technology provide new opportunities for young people’s learning and growth, but it can also expose them to new types of risks.

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life.

Any issues and concerns with online safety must follow Dusemond’s safeguarding and child protection processes.

# Purpose

This policy is implemented to protect the whole Dusemond community. The purpose of the policy is to:

* Ensure the safety and wellbeing of young people when adults or students are using the internet, social media or mobile devices
* Set out expectations for all Dusemond community members’ online behaviour, attitudes and activities and use of digital technology, in and outside of a centre
* Ensure that Dusemond operates in line with its values and within the law in terms of how online devices are used
* Facilitate the safe, responsible, respectful and positive use of technology to support teaching and learning Create an environment that maximises the likelihood that children inform a trusted adult if they feel vulnerable or uncomfortable about online interactions or content
* Help staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
* for the protection and benefit of the young people in their care, and
* for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
* Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.

# Scope

This policy applies to all members of the Dusemond community including staff, students, group leaders and any visitors with access to the systems used by Dusemond at its centres.

# 1.3 Classification of online risks

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

**Content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

**Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

**Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and / or pornography, sharing other explicit images and online bullying; and

**Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If students or staff are at risk, it should be reported to the [Anti-Phishing Working Group](https://apwg.org/contact-us/).

# 2 Roles and responsibilities

To ensure the online safeguarding of members of the Dusemond community, it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as they become apparent.

While this will be a team effort, the following section outlines the online safety roles and responsibilities of individuals and groups within the organisation.

# 2.1 Chief Executive Officer and Director of Operations

The Chief Executive Officer and Director of Operations together have a responsibility to ensure that partner schools and universities have appropriate and effective filtering and monitoring systems in place. Similarly, they are responsible for ensuring that this policy is implemented effectively and reviewed, as a minimum, on an annual basis.

# 2.2 Designated Safeguarding Lead

The designated safeguarding lead takes lead responsibility for day-to-day safeguarding and child protection. This includes responsibility for online safety and understanding of the school’s filtering and monitoring systems and processes.

Their responsibilities include but are not limited to:

* Being aware of the potential for serious safeguarding issues to arise from sharing of personal data, access to illegal/inappropriate materials, inappropriate online contact with adults/strangers, potential or actual incidents of grooming, online bullying
* Ensuring that all staff undergo safeguarding and child protection training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures
* Keeping up to date on current online safety issues and updates in online safeguarding and legislation
* Reviewing and updating this policy and other online safety documents
* Promoting an awareness of and commitment to online safety throughout the Dusemond community Ensuring all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident

# 2.3 All staff

The key responsibilities are:

* To read and follow this policy in conjunction with Dusemond’s main Safeguarding and Child Protection Policy
* To understand that online safety is a core part of safeguarding and everyone’s responsibility
* To record online safety incidents/concerns in the same way as other safeguarding incidents/concerns
* To prepare and check all online sources and classroom resources before using for accuracy and appropriateness
* To take a zero-tolerance approach to all forms of (online) child-on-child abuse, this includes bullying, sexual violence and harassment
* To model safe, responsible and professional behaviours in your own use of technology. This includes outside core centre hours and on social media, in all aspects upholding the reputation of Dusemond and of the professional reputation of all staff
* To notify the designated safeguarding lead if this policy does not reflect practice in centre and follow escalation procedures if concerns are not promptly acted upon

# 2.4 Students

Responsibilities include but are not limited to:

* Adhering to Dusemond’s rules on acceptable use of IT including laptops, mobile phones and tablets
* Understanding the importance of reporting abuse, misuse or access to inappropriate materials including any concerns about a member of Dusemond staff
* Knowing what action to take if they or someone they know feels worried or vulnerable when using online technology, at a Dusemond centre home or anywhere else
* Understanding the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies

# 3 Student acceptable use statement

Students taking part in a Dusemond programme will have access to partner schools’ IT facilities including its PCs and WiFi network in addition to their own devices and 3G, 4G and 5G networks.

Digital technologies have become integral to the lives of children and young people These technologies are powerful tools, which open up new opportunities for everyone and can stimulate discussion and promote creativity and effective learning. Young people are entitled to safe access to these digital technologies.

This Online Safety Policy and this student acceptable use statement is intended to ensure that:

* Students will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
* Dusemond’s and a partner school’s systems and users are protected from accidental or deliberate misuse that could put the security systems at risk

# 3.1 Students’ own personal safety

For their own personal safety students:

* Understand that their use of the school’s systems and devices will be monitored
* Will keep their username and password safe and secure – and will not be shared, nor will they attempt to use another person’s username or password
* Will be aware of ‘stranger danger’ when communicating online and if contacted by someone they don’t know online, will tell a trusted adult
* Will not share personal information about others when online (names, addresses, telephone numbers, email addresses, age, gender, financial details)
* Will take care when sharing information about themselves when online (names, addresses, telephone numbers, email addresses, age, gender, financial details)
* Will not arrange to meet people offline with whom they have communicated online
* Will immediately report any unpleasant or inappropriate material, images, messages or anything that makes them feel uncomfortable

#

# 3.2 Respect for and the safety of others

For the safety of others, students:

* Will be polite and respectful when communicating online and not use aggressive, rude or discriminatory language
* Will not take or send images of other people without their permission

# 3.3 Responsible use of school and Dusemond IT

Students:

* Will not use the school systems or devices for online gambling, online dating, file sharing, or video broadcasting
* Will not try unless I have permission to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
* Understand that the school systems and devices are primarily intended for educational use and won’t be used for personal or recreational use during lessons
* Will not open any hyperlinks in emails or any attachments to emails unless they know and trust the person/organisation who sent the email
* Will not install or attempt to install or store programmes of any type on any school or Dusemond device, nor will they try to alter computer settings

# 4 Staff acceptable use statement

All Dusemond staff have the same responsibilities to use Dusemond IT and partner schools’ IT facilities and digital technologies responsibly and safely. This applies to the central team and those working at Dusemond centres. This policy and staff acceptable use statement is intended to ensure that:

* Staff will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
* Dusemond’s and a partner school’s systems and users are protected from accidental or deliberate misuse that could put the security systems at risk

# 4.1 Professional and personal safety

For their professional and personal safety, staff:

* Understand that their use of digital technology and communication systems will be monitored
* Understand that Dusemond and partner schools’ digital technology systems are primarily intended for work and educational use. Personal and recreational use should only be incidental and take place mainly outside of normal working hours and in any event must not interfere with work commitments
* Will not disclose their username or password to anyone else, nor will they try to use another person’s username or password
* Must follow any password guidelines issued by Dusemond or a partner school and in any event should be difficult to guess, not used for other accounts, nor written down where it may be stolen
* Understand that when leaving their workstation or laptop, the device must be locked to prevent unauthorised access
* Will immediately report any illegal, inappropriate or harmful material or incident they become aware to the Director of Operations or DSL

# 4.2 Responsible use of school and Dusemond IT

Staff:

* Will not access, copy, remove or otherwise any other user’s file with their express permission
* Will communicate with others in a professional manner
* Understand that any email message or technology-based communication which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief, or is defamatory is not permitted and may lead to disciplinary action
* Understand that anything in an email or technology-based communication may be disclosable under data protection regulations
* Will only take and/or publish images of others with their expression permission and in accordance with any ‘images policy’ in force from time to time
* Will only communicate with students, parents/guardians, agents, group leaders using official Dusemond or partner school systems – any such communication will be professional in tone and manner
* Will not engage in any online activity that may compromise their professional responsibilities or bring Dusemond or a partner school into disrepute
* Understand that when using personal mobile devices on Dusemond business, they must follow this policy in the same way as if they were using Dusemond or a partner school’s equipment
* Will not open any hyperlinks or attachments unless the source is known and trusted, or if they have concerns about the validity of the email
* Will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
* Will not try to use any software or method to bypass the filtering/monitoring/security systems in place
* Will not try to make large downloads or uploads that may take up capacity and so prevent others from carrying out their work
* Will not install or attempt to install programmes of any type on any Dusemond or partner school device without the express permission of the Director of Operations, nor will they attempt to alter computer or network settings with permission
* Understand any staff or student data will be kept private and confidential except where disclosure is deemed necessary by law or Dusemond policy
* Will report any damage or faults to equipment or software immediately to the Director of Operations

# 5 Responding to online safety incidents, concerns or disclosures

Internal Dusemond channels should always be followed first for reporting and support, especially in response to incidents, which should be reported in line with Dusemond’s Safeguarding and Child Protection Policy. All members of the Dusemond community are encouraged to be vigilant in reporting online safety concerns/incidents in the confidence that issues will be dealt with quickly and sensitively.

Dusemond will actively seek support from external agencies as necessary (eg the Police, NSPCC, local authorities, UK Safer Internet Centre).

# 5.1 Responding to online safety incidents involving students

If a student is worried about anything online or on a device, they are encouraged to tell a trusted adult as soon as possible.

# 5.1.1 Responding to online abuse/child-on-child abuse disclosure

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices. It can happen anywhere online that allows digital communication (e.g. in messaging apps, online chats, voice chat in games, comments on live streaming sites) and may include cyberbullying, emotional abuse, sexting, sexual abuse/exploitation/harassment and grooming.

Dusemond will respond to concerns and disclosures regarding child-on-child (online) abuse regardless of whether the incident took place in or outside of a centre, using Dusemond/partner school devices or personal devices.

Staff members have the understanding that a student may be reluctant to speak out about abuse they have experienced online. Every disclosure will be taken seriously and staff will always make the student feel supported and not feel ashamed or given the impression that they are causing problems. When responding to cases of online abuse, Dusemond will consider the impact it can have on the student’s wellbeing and provide the child with the right counselling/pastoral support.

If it is believed that the student pupil is in immediate danger, the police need to be contacted on 999. If the student is not in immediate danger, the DSL/DDSL must be informed of any online safety concerns and the school’s child protection procedures will be followed in line with the Dusemond’s Safeguarding and Child Protection Policy.

Parents/group leaders will be informed about cases of online abuse unless to do so would put a child at further risk of harm.

# 5.1.2 Incident of student misuse

Any allegation, concern or suspicion that a student has been involved in any of the following should be reported immediately to Centre Director and DSL and action will be taken in accordance with the Dusemond’s Safeguarding and Child Protection Policy and Behaviour Policy:

* Possession of, or access/attempted access to a website containing images of child abuse
* Possession of, or access/attempted access to a website containing illegal (e.g. obscene or criminally racist) or terrorist or extremist material
* Any incident by electronic means involving ‘grooming’ behaviour
* Any other incident (which may include instances of upskirting or sharing of nudes/semi-nudes) that suggests that a student or another child has suffered or is at risk of suffering serious harm

Concerns or allegations regarding other technology related illegal activity should be reported to the Centre Director. Such concerns will be managed in accordance with the school’s Behaviour Policy although referrals may be made to outside agencies as appropriate.

# 5.1.2.1 Responding to nudes/semi-nudes incidents (sexting)

The production and distribution of sexting images involving anyone under the age of 18 is illegal and needs very careful management for all those involved.

Staff should **immediately** report any incident to the Designated Safeguarding Lead and follow the below [UKCIS Sharing Nudes and Semi-Nudes: How to Respond to an Incident](https://assets.publishing.service.gov.uk/media/65d62d63188d77001103885a/sharing_nudes_and_semi_nudes_how_to_respond_to_an_incident_summary.pdf) (Appendix 1).

* **Never** view, copy, share or save the imagery yourself or ask a child to share or download – this is illegal
* If you have already viewed the image accidentally because you were shown it before you could tell the young person not to show you, report this to the DSL and seek support
* **Do not** delete the imagery or ask the young person to delete it
* **Do not** ask the child/children involved in the incident to disclose information about the imagery – this is the role of the DSL
* **Do not** share information about the incident with other members of staff, the young person(s) involved, or their parents/group leaders
* **Do not** do or say anything that blames or shames the young person(s) involved
* **Do** explain to them that you need to report it and reassure them that they will receive support

The sharing of nudes or semi-nudes may constitute a criminal offence and will be considered in accordance with the Dusemond’s Safeguarding and Child Protection Policy and advice published by the UK Council for Child Safety: ‘Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People’. The DSL will decide next steps and whether other agencies need to be involved. Incidents involving the sharing of nudes and semi-nudes will be recorded on the school’s online incident log.

# 5.1.2.2 Upskirting incident

Upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education.

# 5.1.2.3 Cyberbullying incident

Any allegation of cyberbullying should be reported to the DSL as soon as possible.

#

# 5.2 Procedures for dealing with online safety incidents involving staff

Any allegation, complaint, concern or suspicion that a member of staff has been involved in any of the following should be reported immediately to the DSL and Director of Operations:

* Possession of, or access/attempted access to websites containing images of child abuse
* Possession of, or access/attempted access to a website containing, illegal (e.g. obscene or criminally racist) or terrorist or extremist material
* Any incident by electronic means involving ‘grooming’ behaviour
* Any other incident (e.g. sharing of nudes/semi-nudes) that suggests that a student or another child has suffered or is at risk of suffering serious harm from a member of staff

Concerns or allegations regarding other technology related illegal activity such as fraud, copyright theft or unlawful use of personal data should be reported in line with Dusemond’s Whistleblowing Policy. Any other unsuitable activity or access to unsuitable materials should be reported to the DSL, who will act as appropriate in accordance with the Dusemond’s disciplinary procedures.

Please also refer to the Neutral Notification Guidance. Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).

# 6 Social media

All members of the Dusemond community are expected to engage in social media in a positive, safe and responsible manner and to be mindful when publishing thoughts, concerns, pictures and messages.

# 6.1 Personal use of social media – staff

Staff:

* Are advised that their online conduct on social media can have an impact on their role and reputation within the setting
* Are aware that disciplinary action may be taken if staff are found to bring the profession or Dusemond into disrepute
* Are advised to safeguard themselves and their privacy when using social media sites
* Are encouraged to carefully consider the information (including text and images) they share and post online
* Are aware that information and content that they have access to as part of their employment will not be shared and discussed on social media sites
* Will notify the designated safeguarding lead (DSL) immediately if they consider that any content shared on social media conflicts with their role (Neutral Notification)
* Are advised not to communicate with or add as ‘friends’ any students or their family members
* Any communication from students received via their personal social media accounts should be reported to the DSL

# 6.2 Personal social media use – students

Students are advised:

* To use social media sites which are appropriate for their age
* To consider the benefits and risks of sharing personal details (including personal photos) on social media sites which could identify them and/or their location
* To only approve and invite known friends on social media sites and to deny access to others by keeping online profiles private
* To not post or send images or videos of others without their permission
* To block and report unwanted communications
* To report concerns
* To not send friend requests to Dusemond staff