ONLINE SAFETY POLICY

Publication date:

Review date: 10/01/27

The latest version of this policy is available on the The IDEAL Alliance website and upon request.

Governors have had oversight of this policy and review and approve it annually.

This policy has been produced through collaboration with students, staff, and parents.

Contents

1. Introduction

The IDEAL Alliance is committed to a whole-The IDEAL Alliance approach to online safety and safeguarding that protects and educates students and staff in their technology use. We aim to ensure the online safety of pupils, staff, volunteers, and governors. We use training, education, and effective procedures to educate, empower and protect the whole The IDEAL Alliance community when they are online. We recognise that the use of technology has become a significant component of many safeguarding issues, including child-on-child abuse. We take any concerns seriously and escalate these where appropriate.

In line with Keeping Children Safe in Education, we aim to address the following four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **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:** 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 you feel your pupils, students or staff are risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The DSL takes lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. The DSL liaises with all staff on matters of safety, safeguarding and welfare, including online and digital safety and when deciding upon a referral to relevant agencies.

We strive to consistently create a culture that incorporates the principles of online safety across all elements of The IDEAL Alliance life. This helps to support our safeguarding culture.

The purpose of this policy is to ensure the safety and wellbeing of children when online and provide our staff and volunteers with the guidance and means to do this.

Our mechanisms to identify online safety concerns include our filtering and monitoring system, the direct work we conduct with pupils through our curriculum and the training we provide to staff.

Where online safety concerns arise we utilise our Safeguarding Policy, Acceptable Use Agreements and Behaviour Policy as necessary to ensure an appropriate response. This could include but is not limited to:

- intervention work with pupils on online safety,
- adjustments to the curriculum to teach key ideas or strategies for staying safe online,
- the use of the Behaviour Policy,

Where necessary, we may need to escalate concerns around online safety. The Designated Safeguarding Lead would take a part in this decision-making process and where necessary external agencies would be involved.

2. Roles and responsibilities

2.1 The governing body:

- Take overall responsibility for this policy and its implementation
- Read, and understand this policy
- Ensure the policy is reviewed and updated annually
- Ensure students are taught about online safety
- Ensure staff and governors receive safeguarding training that includes online safety at induction, and that this is regularly updated
- Ensure online safety is a running and interrelated theme whilst devising and implementing the whole The IDEAL Alliance approach to safeguarding and related policies and procedures
- Ensure there are appropriate filtering and monitoring systems in place and regularly review the effectiveness of these systems

2.2. CEO/Heads of School

- Ensure staff understand this policy
- Ensure the implementation of this policy is consistent across the The IDEAL Alliance
- Ensure any new members of staff learn about our approach to online safety at induction and regularly thereafter
- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns

2.3 Designated Safeguarding Lead:

- Support the headteacher in implementing this policy
- Oversee the annual review of the The IDEAL Alliance's approach to online safety, supported by the annual risk assessment that considers and reflects the risks that children face online.
- Take the lead responsibility for online safety as part of their duties as safeguarding lead
- Work with SLT to address any online safety concerns or incidents, in line with our child protection and safeguarding policy
- Liaise with external safeguarding partners as necessary, including children's social care and the police and make referrals with the support of relevant colleagues and their expertise
- Ensure any online safety incidents are recorded appropriately and that staff are aware of how to record online incidents
- Deliver staff training on online safety
- Provide regular updates regarding online safety incidents to the headteacher
- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received

2.4 Network/ICT Manager/IT provider

- Ensure appropriate filtering and monitoring systems are put in place
- Regularly review the filtering and monitoring systems to ensure students are safe from harm online
- Ensure that the The IDEAL Alliance's ICT systems are secure and protected against viruses and malware
- Ensure that the The IDEAL Alliance has an appropriate level of security protection and that this is reviewed periodically to keep up with evolving cyber-crime technologies.

- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received

2.5 All staff and volunteers

- Read and understand this policy
- Assist with the consistent implementation of this policy
- Agree with and follow our acceptable use of IT agreement
- Agree with and follow the Staff Code of Conduct which outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.
- Refer any online safety safeguarding concerns to the DSL or a Deputy DSL by emailing.
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, maintaining an attitude of 'it could happen here' and not dismissing any reports.
- Update parents around what their children are being asked to do online, including the sites they may be asked to access and who, if anyone, their child should be interacting with from the The IDEAL Alliance online.

2.6 Parents

- Understand the importance of children being safe online
- Read, understand and comply with this policy
- Read the information shared with parents regarding acceptable use, what the The IDEAL Alliance asks the child to be doing online, including the sites they will be asked to access and who from the The IDEAL Alliance (if anyone) will be interacting with their child
- Notify a member of staff regarding any questions regarding this policy and its implementation
- Ensure their child has read, understood and agreed to the acceptable use of IT agreement
- Support their child to behave safely and appropriately online

3. Teaching online safety

In line with 'Teaching online safety in School,' published by the Department for Education in January 2023, we teach pupils about online safety and harms in an age appropriate way. Our teaching covers the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. These skills are covered in Computing/PSHE/ RSE/Citizenship/assemblies and group time depending on the age of the child.
Throughout this, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives, including:

- how to evaluate what they see online
- the risks posed by social media platforms
- how to recognise techniques used for persuasion
- unacceptable online behaviour
- how to identify online risks
- how and when to seek support
- how elements of online activity could adversely affect a pupil's personal safety or the personal safety of others online
- how elements of online activity can adversely affect a pupil's wellbeing

Pupils with SEND

We recognise that there are some pupils, for example those with special educational needs, who may be more susceptible to online harm. Such groups may also face additional risks, for example from bullying, grooming and radicalisation. We tailor our curriculum to meet the needs of these pupils by responding to any community needs as they arise. We will ensure these pupils receive the information and support they need through our well designed curriculum.

In addition, our The IDEAL Alliance completes an annual risk assessment for online safety for each school. We consider the updated non-statutory guidance (Jan 2023) from the DfE on teaching online safety and how we teach these elements.

4. Filtering and monitoring

The IDEAL Alliance uses Soltech IT to manage our filtering and monitoring system at Yealmpstone Farm and Ham Drive and SWGfL at Plym Bridge . This filters and monitors for any inappropriate material. This covers our The IDEAL Alliance network and all devices used within it.

The DSL has lead responsibility for understanding the filtering and monitoring systems and processes in place. The DSL and deputies monitor the effectiveness of this system through termly meetings. The DSL is supported by a governor in executing this duty.

The IDEAL Alliance takes care to not 'over block; content so that there are not unreasonable restrictions on what students can be taught regarding online safety.

The processes we have in place have been informed by our risk assessment as required by the Prevent Duty.

The DfE has published filtering and monitoring standards which set out that The IDEAL Alliances should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Review filtering and monitoring provision at least annually
- Block harmful and inappropriate content without reasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet their safeguarding needs

When the filtering and monitoring system detects concerning usage, we will record this XXX and take appropriate action, including a referral to children's social care when necessary.

For more information on filtering and monitoring, parents and carers can contact the head of School for their child's organisation.

5. Security

THE IDEAL ALLIANCE has appropriate levels of security protection, and this is reviewed periodically to keep up with evolving cyber-crime technologies.

6. Educating parents about online safety

We recognise that parents can play a significant role in keeping their children safe online. To raise parents' awareness of online safety, we regularly post information to enable them to understand how to keep their children safe.

7. Acceptable use agreement

All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the The IDEAL Alliance's ICT systems and the internet. Visitors will be expected to read and agree to The IDEAL Alliance's terms on acceptable use if relevant. For further information on acceptable use please refer to the separate agreements which detail our policy on personally owned devices, their use on premises and what is acceptable.

Any breaches of this agreement can lead to further investigation from the leadership of our alliance.

8. Use of mobile and smart technology

We recognise that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at The IDEAL Alliance, can sexually harass, abuse, bully or control their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. To manage this and reduce risk, we only allow Y5 and Y6 children to have a phone and this must be handed into the office/class on arrival and collected on departure. We also support parents if an issue occurs at home.

Our Staff Code of Conduct outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.

In summary in relation to tablets, game, consoles, mobile phones and wearable technology we outline the following for each group:

Staff

Nurseries:

Cannot use mobile phones anywhere where children are. Mobile phones can only be used in the staffroom. Smart devices cannot be worn on a person where children are.

School:

Mobile devices should not be used where children are unless they are being used for school purposes eg. on a school trip. The school reserves the right to check devices at any time.

Pupils

Any mobile phone brought into school must be handed in to the office or class teacher.

Parents

Mobile phones can only be used to record video or photos if all children in the room have permission. Parents can only display images/video of their own child and no-one else's.

In terms of the appropriate use of social media, we outlined the following for each group:

Staff

Staff are encouraged not to befriend any parents. Their accounts must be private. Staff must not befriend children online.

Pupils

None of our children are old enough to be using social media and we remind them of this frequently.

Parents

Parents must not make any negative comments about the school on social media.

9. Training and staff knowledge

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. This will also include training on the filtering and monitoring system used by the The IDEAL Alliance and an understanding of expectations, applicable roles and responsibilities in relation to this.

All staff members will receive refresher training at least annually as part of our safeguarding training programme, as well as regular updates where relevant (for example through emails, e-bulletins and staff meetings).

The DSL and Deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually. This will equip staff with the relevant knowledge and skills to safeguard children effectively, including online.

All staff should be aware and know:

- The indicators of abuse and neglect understanding that children can be at risk of harm inside and outside of the The IDEAL Alliance/college, inside and outside of the home and online.
- To take reports of online harmful behaviour seriously and report them according to the The IDEAL Alliance procedures.
- That technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline.
- That children can abuse other children online, this can take the form of:
    - Online abuse, including sexual
    - Online harassment, including sexual
    - Cyberbullying
    - Misogynistic/ misandrist messages,
    - the non-consensual sharing of incident images, especially around chat groups,
    - and the sharing of abusive images and pornography to those who do not want to receive such content.
    - That child-on-child abuse could be happening in the The IDEAL Alliance setting and that this could be taking place online. All incidents of child-on-child abuse should be reported in line with our reporting systems.

More information about safeguarding training is set out in our child protection and safeguarding policy.

10. Anti-Bullying and child-on-child abuse

We recognise that our approach to online safety should strengthen the work we do around anti-bullying. The anti-bullying approach of The IDEAL Alliance is part of our culture and we ensure we build this into our curriculum in an age appropriate way.

Our work on online safety helps to tackle bullying.

In addition, we understand that online behaviour can also constitute child-on-child abuse. We respond to incidents of child-on-child abuse in line with our Safeguarding Policy and Behaviour Policy.

11. Further information to support you

We work with our local safeguarding partners to ensure our students are safeguarded. We will liaise with these partners where there are safeguarding concerns and will follow their policies and procedures when needing their support. This may include referrals or seeking advice from Children's Social Care, our local Prevent team and/ or the police.

For **parents** the following websites could be of use:

- Samaritans: Talking to your child about self-harm and suicide content online
- NSPCC Online Safety Guides for parents
- Report harmful content at https://reportharmfulcontent.com/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/
- CEOP - how to help your children get the most out of the internet
- Further guidance shared by the DfE can be accessed here

For **students** the following websites could be of use:

- Mind- mental health support
- Togetherall- online community accessible 24/7
- Shout- a free text service available 24 hours a day. You can start a conversation by texting Shout to 85258
- Samaritans' self-help app
- Kooth is an online mental wellbeing community for young person
- Report harmful content at https://reportharmfulcontent.com/child/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/

For **all staff and volunteers** it is useful to be aware of the resources available to staff and students so that you can signpost them as required. In addition, the following resources could be of use:

- UK Safer Internet Centre- practical resources, advice, and training to support safe and responsible internet use.
- internetmatters.org – research, free lesson plans, and resources to support the teaching of online safety and digital literacy across subject areas.
- DfE guidance Teaching online safety in The IDEAL Alliances - non-statutory guidance outlining how The IDEAL Alliances can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

Policies/ guidance to be read and understood alongside our online safety policy:

- Safeguarding/ Child Protection policy.
- Behaviour policy.
- Staff Code of Conduct inc. acceptable use of technology in the staff behaviour policy/ code of conduct.

- Anti-bullying procedures including cyberbullying
- The Prevent Duty and The Prevent duty: an introduction for those with safeguarding responsibilities
- Meeting digital and technology in The IDEAL Alliances and colleges (DfE)

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: ● Ask a teacher or adult if I can do so before using them. ● Only use websites that a teacher or adult has told me or allowed me to use. ● Tell my teacher immediately if: ○ I click on a website by mistake. ○ I receive messages from people I don't know. ○ I find anything that may upset or harm me or my friends. ● Use school computers for schoolwork only. ● Be kind to others and not upset or be rude to them. ● Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly. ● Only use the username and password I have been given. ● Try my hardest to remember my username and password. ● Never share my password with anyone, including my friends ● Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer ● Save my work on the school network. ● Check with my teacher before I print anything. ● Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** ● Always use the school's ICT systems and the internet responsibly and for educational purposes only ● Only use them when a teacher is present, or with a teacher's permission. ● Keep my usernames and passwords safe and not share these with others. ● Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer ● Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others. ● Always log off or shut down a computer when I've finished working on it **I will not:** ● Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity. ● Open any attachments in emails, or follow any links in emails, without first checking with a teacher. ● Use any inappropriate language when communicating online, including in emails. ● Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate. ● Log in to the school's network using someone else's details. ● Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision. **If I bring a personal mobile phone or other personal electronic device into school:** ● I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission. ● I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the school's reputation. ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services. ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network. ● Share my password with others or log in to the school's network using someone else's details. ● Take photographs of pupils without checking with teachers first ● Share confidential information about the school, its pupils or staff, or other members of the community. ● Access, modify or share data I'm not authorised to access, modify or share. ● Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
ONLINE SAFETY TRAINING NEEDS AUDIT	
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	
Signed:	**Date:**

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**