DANES EDUCATIONAL TRUST

ONLINE SAFETY POLICY
The Beaconsfield School

RESPONSIBILITIES	
To determine and approve policy and ensure compliance	DET Central Services Team
To implement, deliver and comply	Headteacher
APPROVAL DATE	1 May 2026
COMMITTEE	n/a DET COO
DURATION	Annual
REVIEW DATE	Autumn 2026
TRUST / SCHOOL LEAD	Head of IT / Caroline Legg
As part of the review process, this policy/procedure has been subject to an Equality Impact Assessment.	

Contents

1. AIMS 3
2. LEGISLATION AND GUIDANCE 3
3. ROLES AND RESPONSIBILITIES 4
4. EDUCATING PUPILS ABOUT ONLINE SAFETY 6
5. EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY 8
6. CYBER-BULLYING 8
7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL 10
8. PUPILS USING MOBILE DEVICES IN SCHOOL 10
9. STAFF USING WORK DEVICES OUTSIDE SCHOOL 10
10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE 11
11. TRAINING 11
12. MONITORING ARRANGEMENTS 12
13. LINKS WITH OTHER POLICIES 12
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) ... 13
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers) 13
Appendix 3: acceptable use agreement (staff, governors, volunteers) 14
Equality Impact Assessment Form 15

1. AIMS

The Beaconsfield School (the School) recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff, governors and trustees will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues. We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of our pupils.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching

for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

3. ROLES AND RESPONSIBILITIES

The Trust Board

The Trust board has overall responsibility for monitoring this policy and ensuring each school board and headteacher is held to account for its implementation. Through delegation to the headteacher the Trust Board will:

Make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

Will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

Will coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

Will ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Trust must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The trust board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

Online Safety will be considered as part of the Trust Safeguarding Committee, a committee of the Trust Board.

All Trustees and governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The headteacher

The headteacher is responsible for ensuring that staff and volunteers understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Trust safeguarding lead to discuss online safety incidents as part of termly reports and annual review
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Trust Head of IT to make sure the appropriate Monitoring and filtering systems are in place
- Working with the headteacher, Trust Head of IT and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on the schools online child protection system and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the behaviour and Anti-bullying policies
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or school board
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The Network Administrator

The Network Administrator or where 3rd Party IT support is in place the Regional IT Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are flagged to the DSL
- Ensuring that any incidents of cyber-bullying are reported to the DSL

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by raising a concern with the DSL via CPOMS
- Following the correct procedures of contacting the DSL if there is a request to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour and anti-bullying policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

pUPILS will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **KS3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website.

This policy will also be shared with parents/carers via our school website.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. CYBERBULLYING

Cyberbullying can take many forms and can go even further than face-to-face bullying by invading personal space and home life, and can target more than one person. It can also take place across age groups and target pupils, staff and others, and may take place inside school, within the wider community, at home or when travelling. It can sometimes draw bystanders into being accessories. Cyberbullying is covered in our Anti-Bullying Policy and is treated in the same way as any other form of bullying.

In relation to a specific incident of cyberbullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider any response in line with the Child Protection and Safeguarding Policy. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, this should be raised with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Child Protection and Safeguarding Policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, this is the same as with any other new online resource.

Any use of artificial intelligence should be carried out in accordance with our AI policy.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils may bring mobile devices into school, but they must be locked away in their Yondr pouches are not permitted to use them during the school day unless there is an approved medical need. Pouches can be unlocked and phones can be used only on leaving the school site.

9. STAFF USING WORK DEVICES OUTSIDE SCHOOL

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT Administrator.

10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. TRAINING

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.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:

- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety every 2 years as part of their DSL refresher training. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

The school will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

12. MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety on the schools online child protection system.

This policy will be reviewed every year by the Trust Head of IT and also the Trust Safeguarding Lead.

13. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Trust AI Policy

Appendix 1: KS3 and KS4 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 that 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 am permitted to bring a personal mobile phone or other personal electronic device into school in accordance with section 8 above:** ● 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:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
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, AND VOLUNTEERS .
Name of staff member/governor/volunteer:
You must read this agreement in conjunction with the Online Safety policy, Data Security Policy and the Data Protection Policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities. Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff are aware of their responsibilities in relation to their use. All staff are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the e-safety coordinator, DSL or ICT Team. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.
Internet Access I will not access, attempt to access or share any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed. **Online conduct** I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute. I will not browse, share, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion. I will report any accidental access to or receipt of inappropriate materials or filtering breach to the e-safety coordinator or DSL. I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required as part of an internal investigation, must be made available to my line manager, headteacher or data protection officer as required. I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, AND VOLUNTEERS .

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with anyone as outlined in the data security policy.

Data protection

I will follow requirements for data protection as outlined in Data Protection policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body
- Personal or sensitive data taken off site or outside of school systems must be encrypted

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, AND VOLUNTEERS .

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the GDPR. I will not use my school email addresses for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices unless a closed, monitorable system has been set up by the school.

External Hard drives and USB Sticks

The use of External Hard drives and USB Sticks is at the discretion of the Headteacher and may not be allowed. Where allowed these devices must be encrypted at all times otherwise school approved cloud storage or school network storage should be used.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the ICT Team and, if required, after having completed the required form: Sharing personal data with a new organisation.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, AND VOLUNTEERS .	
Promoting online safety I understand that online safety is the responsibility of all staff and I will promote positive online safety messages at all times including when setting homework or providing pastoral support. I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, pupils or parents/carers) to the DSL. **Classroom management of internet access** I will pre-check for appropriateness all internet sites or online videos used in the classroom and for remote learning; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the e-safety coordinator	
Signed (staff member/governor/volunteer):	**Date:**

Equality Impact Assessment Form

People responsible for overseeing the EIA
Trust Head of IT
Name of the policy, procedure or project
Online Safety Policy
What is the main purposes or aims of the policy, procedure or project?
To ensure all pupils, staff & parents are aware of how to stay safe online and the processes the school follows.
Who will be the beneficiaries of the policy, procedure or project?
All stakeholders.
Have you consulted on this policy, procedure or project?
Yes, with all network administrators, headteachers and also Trust safeguarding Lead, Head of HR and Head of Compliance.

Complete the following table and give reasons/comments for where:

The policy, procedure or project could have a positive impact on any person or group because of one of the following aspects of their identity (this includes equality of opportunity of access)

The policy, procedure or project could have a negative impact on, or disadvantage, a person or group because of one of the following aspects of their identity.

(At this stage, it is important to consider the requirements placed upon a school as per the Equality Act 2010.)

Groups	Positive impact		Negative impact		Comments
	High	Low	High	Low	
Race	x				This policy relates to staying safe online and protects each of the protected characteristics equally.
Religion or belief	x				This policy relates to staying safe online and protects each of the protected characteristics equally.
Sexual orientation	x				This policy relates to staying safe online and protects each of the protected characteristics equally.
Sex	x				This policy relates to staying safe online and protects each of the protected characteristics equally.
Disability	x				This policy relates to staying safe online and protects each of the protected characteristics equally.
Age	x				This policy relates to staying safe online and protects each of the protected characteristics equally.
Gender reassignment	x				This policy relates to staying safe online and protects each of the protected characteristics equally.
Pregnancy and maternity					

Marriage and civil partnership					

Where there is negative impact, what actions could be taken to amend the policy, procedure or project to minimise the negative impact?
If there is no evidence that the policy, procedure or project promotes equality, equal opportunities or improves relationships between people with different protected characteristics, what amendments could be made to achieve this?
How will the policy, procedure or project be implemented including any necessary training?