

# Ditcham Park School



## Online Safety Policy

**Approved by:**

**Date: September 2023**

**Last reviewed on:**

**September 2023**

**Next review due by:**

**September 2024**

# Contents

1. Aims .....	2
2. Legislation and guidance .....	3
3. Roles and responsibilities .....	3
4. Educating pupils about online safety .....	5
5. Educating parents/carers about online safety .....	7
6. Cyber-bullying .....	7
7. Prevent .....	9
8. Acceptable use of the internet in school .....	9
9. Pupils using mobile devices in school .....	9
10. Staff using work devices outside school .....	9
11. How the school will respond to issues of misuse .....	10
12. Training .....	10
14. Monitoring arrangements .....	11
15. Links with other policies .....	11
Appendix 1: Student - Acceptable IT Use Statement and Agreement .....	12
<i>NB: if you have any concerns in respect of your child's ability to comply with the terms of this agreement please contact matthew.mitas@ditchampark.com .....</i>	13
Appendix 2 : Acceptable IT Use Policy - Staff (staff, governors, volunteers and visitors) .....	14
<i>The companies Acceptable IT Use policy outlines all actions that are deemed acceptable and unacceptable within the school, if you would like a copy of this policy please ask a member of the IT Department. ....</i>	14
The company reserves the right to change any policies or procedures as and when it see's fit to do so. ....	14
Appendix 3: Online Incident Report Sample .....	15
Appendix 4: online safety training needs – self-audit for staff .....	16

---

## 1. Aims

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 child to child 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.

## 3. Roles and responsibilities

### 3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing 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.

The governing board 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.

The governing board will co-ordinate 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).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board 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 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 those 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.

The governor who oversees online safety is Linda Campbell

All 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 2)
- › Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college 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

### **3.2 The headteacher**

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

### **3.3 The designated safeguarding lead**

Details of the school's designated safeguarding lead (DSL) and the Deputy are set out in our Child Protection and Safeguarding policy:

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 headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- › Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- › Working with the ICT manager to make sure the appropriate systems and processes are in place
- › Working with the headteacher, ICT manager 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 and dealt with appropriately in line with this policy
- › Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- › 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 governing board
- › Undertaking annual risk assessments that consider and reflect the risks children face
- › 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.

### **3.4 The Network manager**

The Network 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 weekly basis
- › Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- › Ensuring 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 policy

This list is not intended to be exhaustive.

### 3.5 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, 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 emailing the ICT manager and the DSL
- › Following the correct procedures by emailing the DSL and the Network manager for approval if they need to bypass the filtering and monitoring systems for educational purposes
- › Working with the DSL/Network Manager 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 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.

### 3.6 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

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 International](#)
- › Parent resource sheet – [Childnet International](#)

### 3.7 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.

## 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 **Key Stage (KS) 1**, pupils will be taught to:

- › Use technology safely and respectfully, keeping personal information private
- › Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- › Use technology safely, respectfully and responsibly
- › Recognise acceptable and unacceptable behaviour
- › Identify a range of ways to report concerns about content and contact

By the **end of Year 6**, pupils will know:

- › That people sometimes behave differently online, including by pretending to be someone they are not
- › That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- › The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- › How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- › How information and data is shared and used online
- › What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- › How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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 which 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 prison
- › 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

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.

Online safety will also be covered through online webinars.

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. Cyber-bullying

### 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their classes/tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

The headteacher, and any member of teaching staff, 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 the Head of Seniors or the Head of Juniors
- › 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

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

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, it is up to the Headteacher or the Head of Seniors or the Head of Juniors 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 behaviour 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.

## 6.4 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 Bard.

Ditcham Park recognises 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.

Ditcham Park will treat any use of AI to bully pupils in line with our 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.

## 7. Prevent

The Prevent Duty Guidance (2023) places a statutory duty on named organisations, including schools, to have due regard towards the need to prevent people being drawn into terrorism.

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their message. The filtering systems used at Ditcham Park blocks inappropriate content, including extremist content. Where staff or pupils find unlocked extremist content they should follow the procedures set out in the school's Safeguarding / Child Protection Policy and discuss their concerns with the school's designated safeguarding leads (DSLs), without delay.

## 8. 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. 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.

## 9. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day.

All mobile devices from Year 7 upwards must be put in to a Yondr pouch at the start of each day. Pupils are not permitted to take them out until the end of the school day. In the Junior school, all mobile devices are handed in to the class teacher at the start of the school day and are returned at home time.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

## 10. 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

- › 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..

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 network manager.

## 11. 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 in our behaviour policy. 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 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.

## 12. 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, 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 the DDSL 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 on the subject of online safety at regular intervals, and at least annually.

Governors 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.

## **14. Monitoring arrangements**

The DSL/Network Manager logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## **15. Links with other policies**

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Acceptable IT Use Policy - PUPIL
- Acceptable IT Use Policy - STAFF

## Appendix 1: Student - Acceptable IT Use Statement and Agreement

Ditcham Park School has provided students with computers and internet access to help with studies and learning. The rules stated below will help to ensure that all members of the Ditcham community remain safe and free of any undesirable materials whilst using the School's network.

1. I will access the system with the username that has been provided to me by Ditcham Park School; I will also use my own personal password and not give this information to anyone else.
2. I will not access other people's files or accounts for any reason, even if permission has previously been given.
3. I will only use the School computers or Chromebooks for school related work.
4. I will not under any circumstances use any form of Instant Messaging or Online Social Networking.
5. I accept responsibility for all materials held on my personal devices.
6. I will not send any emails or other electronic forms of communications that may cause offence or hurt to others, whether that is the intention or otherwise.
7. I will not give out any personal details, or arrange meetings with anyone, unless permission has been given by a parent, guardian, or teacher.
8. I will report any unpleasant or suspicious materials found while using either the School's network, or the Internet to a member of staff immediately
9. I understand that the School has the right to check my School account and monitor my Internet usage.
10. I will not use offensive or hurtful comments towards the school, its staff or pupils while using the Internet or school systems.
11. I understand that the use of the School's wireless network (Wi-Fi) is reserved for School staff and is not to be used by students, unless authorised by the IT department, except for access for School provided devices. If given permission by the IT Department, policies apply as stated in section 4.3.8 of the Acceptable IT Use Policy.
12. All AI related usage on the Ditcham Park Network or any Ditcham software will adhere to the guidelines laid out in the "Pupil AI Policy".

Please turn over to continue reading the Chromebook specific section of this document.

### Chromebook Specific

This section outlines the School’s expectation for the use of School issued Chromebooks. Your School issued Chromebook remains the property of Ditcham Park School.

#### I agree that:

- I will bring my Chromebook to School every day, unless otherwise instructed.
- I will come to school with my Chromebook fully charged.
- I will inform the IT Department of any damage immediately.
- I will take every precaution not to damage my Chromebook, this includes: Securing your Chromebook in its case when not in use, storing your Chromebook in your school bag when moving between lessons, using your cubby hole outside of lesson time to store your bag/Chromebook.
- I will not touch other pupils’ Chromebooks unless instructed by a teacher.
- My Chromebook is a learning tool, it should only be used for academic studies and research.
- Any damage that occurs as a result of misuse or carelessness on my part could result in my parents/guardians having to contribute to the replacement device, and they will be notified accordingly by the Head of IT or the School Bursar.
- I will use my Chromebook in line with the Ditcham Park School ‘Acceptable IT Use Policy’.

\*\*\*\*\*

I understand that the points made above are meant as a guide. By signing this document, you agree to the terms set out in the Acceptable IT Use Policy. I also understand that these rules are subject to change and that I will conduct myself in a mature and sensible manner when using any item of electronic equipment within the school.

Student Name:

Signed \_\_\_\_\_ Date \_\_\_\_\_

*The School’s Acceptable IT Use Policy outlines all actions that are deemed acceptable and unacceptable within the school, if you would like a copy of this full policy please ask a member of the IT Department.*

*NB: if you have any concerns in respect of your child’s ability to comply with the terms of this agreement please contact [matthew.mitas@ditchampark.com](mailto:matthew.mitas@ditchampark.com)*

## Appendix 2 : Acceptable IT Use Policy - Staff (staff, governors, volunteers and visitors)

### Ditcham Park School Acceptable IT Usage Policy

- The intranet, internet or related cloud-based systems governed by the school are made available to staff to enhance their professional activities, including work accomplishment, research, administration and management. The school's Acceptable IT Use Policy has been drawn up to protect all parties – students, staff and Ditcham Park School.
- The school reserves the right to examine or delete any files that may be held on the Intranet, internet or related cloud-based systems and to monitor any sites visited.
- All internet activity should be appropriate to the employee's job specification; however occasional use of the Internet for personal reasons is acceptable.
- Access should only be made via an authorised school account; this account should not be made available to any other person.
- Activities that threaten the integrity of the school's intranet, internet or related cloud-based systems or an activity that attacks or corrupts other systems is forbidden.
- Users are responsible for all emails sent (both personal and corporate), and for contacts made that may result in the receipt of emails within the school.
- Use of the school systems for personal or financial gain, gambling, political, or advertising purposes is forbidden.
- Copyright materials must be respected.
- Posting of anonymous messages and forwarding chain letters is forbidden.
- As emails can be forwarded or inadvertently sent to the wrong contact, professional levels of language and content should be applied as for all other mediums used.
- Use of the network to access inappropriate materials such as pornographic, racist, or offensive content is forbidden.
- Use of the schools wireless network (Wi-Fi) is allowed for staff providing they have been given authorisation by the IT Department. Policies apply as stated in section 4.2.9 of the Acceptable IT Use Policy.
- All AI related usage on the Ditcham Park Network or any Ditcham software will adhere to the guidelines laid out in the "Staff AI Policy".
- By signing this document you agree to the terms set out in the Acceptable IT Use policy. Also that the conditions stated above are meant as a guide and that these points may be changed at any time to suit the schools needs and requirements.
- 

Full Name Position \_\_\_\_\_

Signed \_\_\_\_\_ Date \_\_\_\_\_

*The companies Acceptable IT Use policy outlines all actions that are deemed acceptable and unacceptable within the school, if you would like a copy of this policy please ask a member of the IT Department.*

**The company reserves the right to change any policies or procedures as and when it see's fit to do so.**

### Appendix 3: Online Incident Report Sample

Checked	Date	UserName	Category	Positive	False Positive	Reported to DSL/DDSI	Reported to	URL	Screenshot Y/N
MM	09/01/2024 09:52	04gallagherj	Self Harm		Y	No		when did harriet westbrook commit suicide - <a href="https://www.google.com/search?q=when+did+harriet+westbrook+commit+suicide&amp;rlz=1CAPQVF_enGB1076&amp;oq=when+did+harriet+westbrook+commit+suicide&amp;gs_lcrp=EgZjaHJvbWUyBggAEEUYOdlBCTEwMjg5ajBqN6gCALACAA&amp;sourceid=chrome&amp;ie=UTF-8&amp;safe=active&amp;ssui=on">https://www.google.com/search?q=when+did+harriet+westbrook+commit+suicide&amp;rlz=1CAPQVF_enGB1076&amp;oq=when+did+harriet+westbrook+commit+suicide&amp;gs_lcrp=EgZjaHJvbWUyBggAEEUYOdlBCTEwMjg5ajBqN6gCALACAA&amp;sourceid=chrome&amp;ie=UTF-8&amp;safe=active&amp;ssui=on</a>	N
MM	11/01/2024 11:56	05droverm	Suicide - Caution		Y	No		<a href="https://www.google.com/search?q=does+sniffing+glue+make+you+feel+nice&amp;gs_lcrp=EgZjaHJvbWUyBggAEEUYOdlBCTM5NTgyajBqN6gCALACAA&amp;sourceid=chrome&amp;ie=UTF-8&amp;safe=active&amp;ssui=on">ce&amp;rlz=1CAPOVF_enGB1087&amp;oq=does+sniffing+glue+make+you+feel+nice&amp;gs_lcrp=EgZjaHJvbWUyBggAEEUYOdlBCTM5NTgyajBqN6gCALACAA&amp;sourceid=chrome&amp;ie=UTF-8&amp;safe=active&amp;ssui=on</a> - does sniffing glue make you feel nice	N
MM	17/01/2024 11:38	04collinsa	Pornography		Y	No		<a href="https://mc.vandex.by">https://mc.vandex.by</a>	N
MM	17/01/2024 12:02	07busuttila	Pornography		Y	No		<a href="https://thechive.com">https://thechive.com</a>	N
MM	18/01/2024 09:18	05morgand	Pornography		Y	No		<a href="https://www.google.com/search?q=what+did+dylan+thomas+experience&amp;sc_esv=599405545&amp;bih=599&amp;biw=1366&amp;rlz=1CADTIH_enGB1085&amp;hl=en-GB&amp;ei=Y-yoZdW4IK-ChbiP_euAsAs&amp;ved=0ahUKEwiV9oalzeaDaxUvOUEAHf01ALYQ4dUDCBA&amp;uact=5&amp;oq=what+did+dylan+thomas+experience&amp;gs_lcp=Egxdnd3Mtd2l6LXNlc_nAilHdoYXOgZGiklGR5bGFuHRob21hcyBleHBicmlmbmNlMgUQRigAUj9kICQa1iWkXABeAGOAOCYAYcDoAHsEKoBCDAuMTIuMC4xuAEDvAFA-AEBwgIKEAAYRxiWBBiwABICCxAAAGIAEGIoFGJECwglFEAAYgATCAgYOABgWGB7CAgsQABiABBiKBRiGA8iCBRAhGJ8FwglHECEYChigAelIDBgAlEGlBgGQBg&amp;scient=gws-wiz-serp&amp;safe=active&amp;ssui=on">https://www.google.com/search?q=what+did+dylan+thomas+experience&amp;sc_esv=599405545&amp;bih=599&amp;biw=1366&amp;rlz=1CADTIH_enGB1085&amp;hl=en-GB&amp;ei=Y-yoZdW4IK-ChbiP_euAsAs&amp;ved=0ahUKEwiV9oalzeaDaxUvOUEAHf01ALYQ4dUDCBA&amp;uact=5&amp;oq=what+did+dylan+thomas+experience&amp;gs_lcp=Egxdnd3Mtd2l6LXNlc_nAilHdoYXOgZGiklGR5bGFuHRob21hcyBleHBicmlmbmNlMgUQRigAUj9kICQa1iWkXABeAGOAOCYAYcDoAHsEKoBCDAuMTIuMC4xuAEDvAFA-AEBwgIKEAAYRxiWBBiwABICCxAAAGIAEGIoFGJECwglFEAAYgATCAgYOABgWGB7CAgsQABiABBiKBRiGA8iCBRAhGJ8FwglHECEYChigAelIDBgAlEGlBgGQBg&amp;scient=gws-wiz-serp&amp;safe=active&amp;ssui=on</a>	N

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

ONLINE SAFETY TRAINING NEEDS AUDIT	
<b>Name of staff member/volunteer:</b>	<b>Date:</b>
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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	



