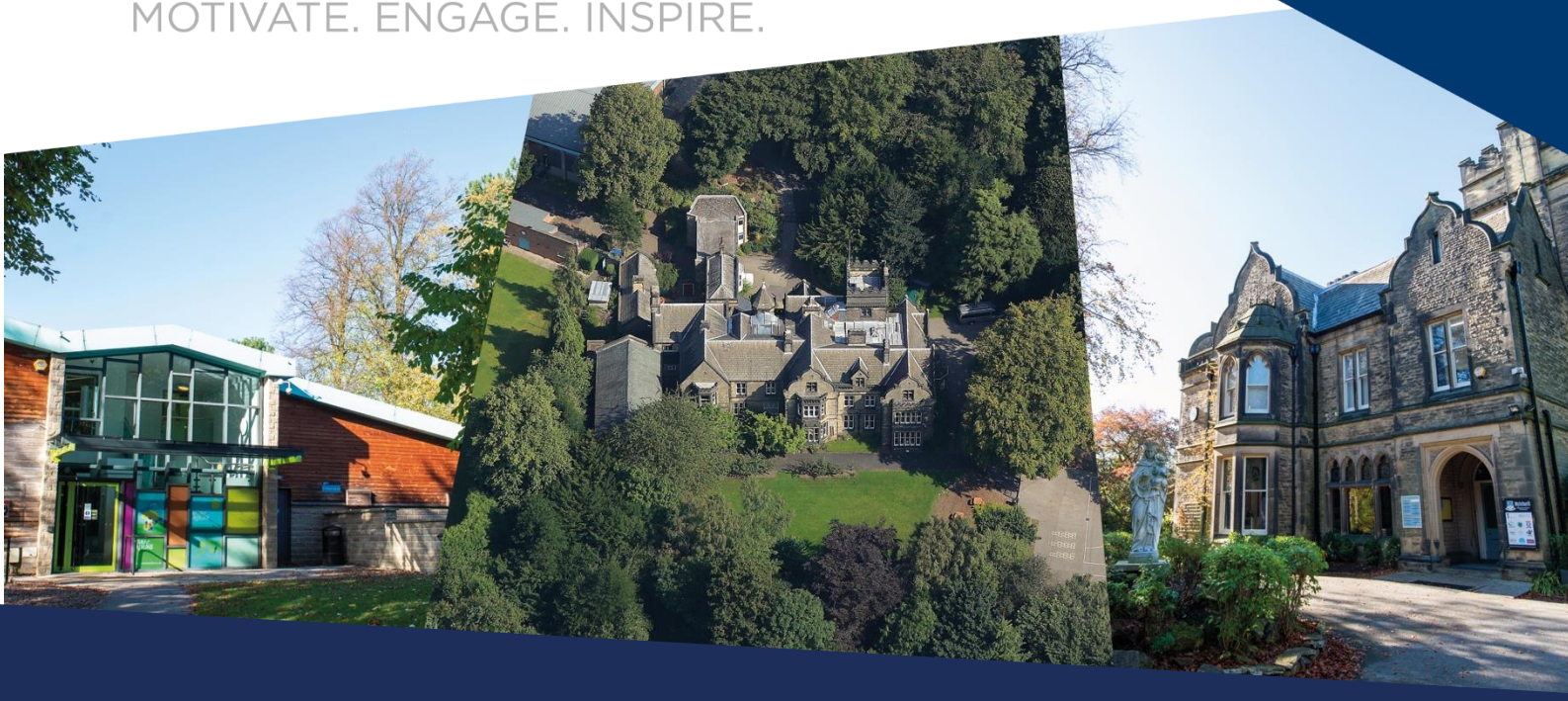
Mylnhurst
Preparatory School and Nursery

MOTIVATE. ENGAGE. INSPIRE.

Mylnhurst Campus Group



Policy Document

Mylnhurst School & EYFS

# Online Safety

Publication Date: September 2021

Review Date: September 2022

| | |
|---|---|
| Approved by SLT | September 2021 |
| Approved by Board of Directors | September 2021 |

## Contents

## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## 2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education 2020, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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 also takes into account the National Curriculum computing programmes of study.

## 3. Roles and responsibilities

### 3.1 The Board of Directors

The Board of Directors has overall responsibility for monitoring this policy.

The Headmistress is responsible for its implementation.

The Board of Directors will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

### 3.2 The Headmistress

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

### 3.3 Designated Senior Persons for Safeguarding

Details of the Designated Senior Persons for Safeguarding 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- 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

This list is not intended to be exhaustive.

### 3.4 The ICT manager

The ICT manager (Bluebox IT) is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 as appropriate
- 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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- 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 policy

This list is not intended to be exhaustive.

### 3.6 Parents

Parents 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 (appendix 1)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

### 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 (appendix 2).

## 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In the EYFS and Key Stage 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 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

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

## 5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Sessions in online safety will also be offered in school to parents and carers on an annual basis.

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

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 one person or group by another person or group, where the relationship involves an imbalance of power. (Cyber-Bullying forms a part of the schools' behaviour and anti-bullying policies

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.

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.

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 distributed among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with other external services where it is deemed necessary.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

## 7. Acceptable use of the internet in school

All pupils, parents, 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 and 2). 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, directors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

## 8. Pupils using mobile devices in school

Under no circumstances are pupils permitted to bring mobile devices on to the school site. Any pupil found with a mobile device will have it removed and returned to parents at the earliest convenience.

## 9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

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

Work devices must be used solely for work activities.

## 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 the 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which 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).

The DSL 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.

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

Volunteers will receive appropriate training and updates, where appropriate.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

## 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMs.

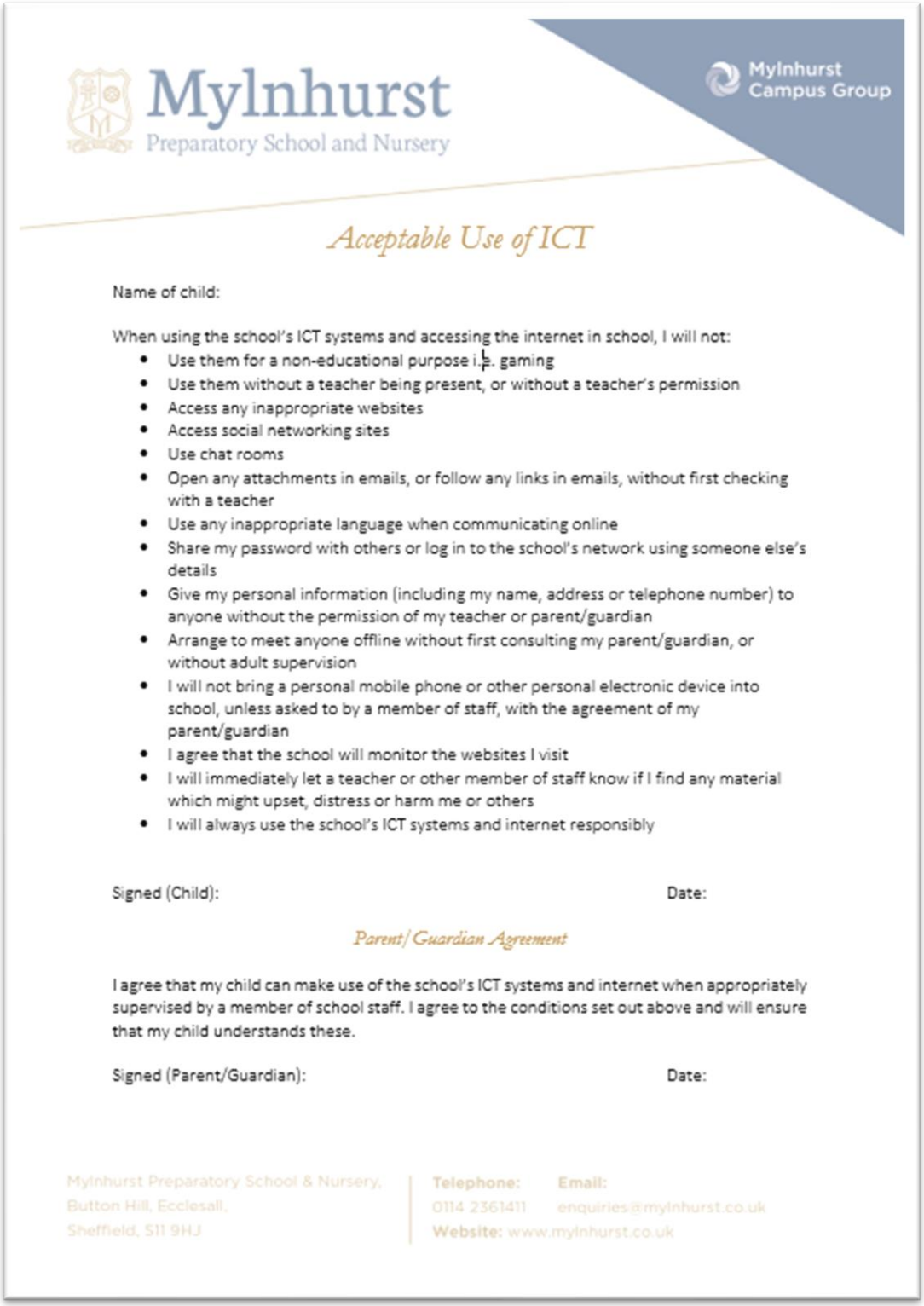
This policy will be reviewed annually by the Designated Safeguarding Leads with Responsibility for Online Safety. The Policy will be scrutinised by the Board of Directors annually.

## 13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints Policy and Procedure

Appendix 1: acceptable use agreement (pupils and parents/guardians).



Mylnhurst
Preparatory School and Nursery

Mylnhurst
Campus Group

## Acceptable Use of ICT

Name of child:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose i.e. gaming
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/guardian
- Arrange to meet anyone offline without first consulting my parent/guardian, or without adult supervision
- I will not bring a personal mobile phone or other personal electronic device into school, unless asked to by a member of staff, with the agreement of my parent/guardian
- I agree that the school will monitor the websites I visit
- I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others
- I will always use the school's ICT systems and internet responsibly

Signed (Child): Date:

### Parent/Guardian Agreement

I agree that my child can make use of the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above and will ensure that my child understands these.

Signed (Parent/Guardian): Date:

Mylnhurst Preparatory School & Nursery,
Button Hill, Ecclesall,
Sheffield, S11 9HJ

Telephone: 0114 2361411
Email: enquiries@mylnhurst.co.uk
Website: www.mylnhurst.co.uk

Appendix 2: acceptable use agreement (staff)

Mylnhurst
Preparatory School and Nursery

Mylnhurst
Campus Group

*Acceptable Use Agreement*

Members of staff

By signing this document, I confirm that I have read and agreed to the points pertaining to the acceptable us of technology within Mylnhurst's Safeguarding Policy, Online Safety Policy and Code of Conduct.

I understand that it is my responsibility to stay up-to-date with the school's policies and procedures and that failure to comply with this agreement could result in disciplinary action.

Name:

Role:

Date:

Signed:

Mylnhurst Preparatory School & Nursery,
Button Hill, Ecclesall,
Sheffield, S11 9HJ

**Telephone:** 0114 2361411
**Email:** enquiries@mylnhurst.co.uk
**Website:** www.mylnhurst.co.uk

Mylnhurst Preparatory School & Nursery,
Button Hill, Ecclesall,
Sheffield, S11 9HJ

**Telephone:** 0114 2361411
**Email:** enquiries@mylnhurst.co.uk
**Website:** www.mylnhurst.co.uk