

Springwell Leeds Academy

E-Safety Policy

Revised March 2021

Scope of the Policy

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. Use of ever more powerful computers, iPads, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At Springwell, we recognise that learning is a lifelong process and that e learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities that are inappropriate, or possibly illegal. E-safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

This policy applies to all stakeholders of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but which are linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Contents

1. Aims	4
2. Legislation and guidance	4
3. Roles and responsibilities	5
4. Educating pupils about online safety	6
5. Educating parents about online safety	7
6. Cyber-bullying	7
7. Acceptable use of the internet in school	8
8. Pupils using mobile devices in school	9
9. Staff using work devices outside school	9
10. How the Academy will respond to issues of misuse	9
11. Training	9
12. Monitoring arrangements	10
13. Links with other policies	10
14. Use of digital and video images - Photographic, Video	10
15. Data Protection	10
16. Communications	11
17. Inappropriate Use	12
18. Remote Learning	13
Appendix 1: Acceptable use agreement (pupils and parents/carers)	14
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)	16
Appendix 3: Online Learning Guide for Parents and Carers	17

1. Aims

Our Academy 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 Academy 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 (DfE) 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 head teachers 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

3.1 The governing board

Governors monitoring of the policy will be supported by some / all of the following:

- Dashboard reports re KPIs at each LGB meeting and follow up 'deep-dive' reports
- Annual staff 'voice' survey
- Annual parent/carer survey
- Regular discussion and review of AIP priorities
- Trust peer review processes
- External perspectives including HT feedback from LA Commissioners
- Benchmarking across the Trust with other SEND provision
- Benchmarking regionally and nationally where appropriate information is accessible
- Link governor reports
- Governor visits (including engagement with staff virtually)

The academy's safeguarding governor is [Carol Stephenson](#).

3.2 The Executive Principal

The Executive Principal 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

Associate Principals / Head of Centre for each site will ensure that each site has sufficient appropriately trained staff in a Designated Safeguarding Lead (DSL) role.

Details of the Academy DSL's and deputy/deputies are set out in the academy's child protection and safeguarding policy as well as staff handbook.

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

- Supporting the Executive Principal in ensuring that staff understand this policy and that it is being implemented consistent Executively throughout the school
- Working with the Associate Principal, ICT support provider 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 Academy Anti-Bullying 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 schools to the Executive Principal and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT Support Provider

The ICT support provider 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 on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 (via Behaviour Watch Sign off) and adhering to the terms on acceptable use of the Academy's ICT systems and the internet (appendix 2), and ensuring that pupils follow the Academy'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 Academy Anti-Bullying Policy.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Executive Principal 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](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the academy'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:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In **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

By the **end of primary school**, 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, 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 **Key Stage 4** 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 which 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

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

5. Educating parents about online safety

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

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

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

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. (See also the Anti-Bullying 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 Academy 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 will discuss cyber-bullying with their 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 (see section 11 for more detail).

The Academy also sends information on cyber-bullying to parents so that 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 Academy will follow the processes set out in the Academy Anti-Bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the Academy 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 external services if it is deemed necessary to do so.

6.3 Examining electronic devices

Academy 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
- Disrupt teaching, and/or
- Break any of the Academy 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), 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](#) and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the Academy 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 (appendix 1). 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.

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

8. Pupils using mobile devices in school

At Springwell Leeds Academy we recognise that students and parents see that having access to a mobile phone is part of modern life and has become an essential way in which parents and carers can keep in touch with pupils on the way to and from the academy. It is important however that the use of the phone does not interfere with learning or cause a distraction or disruption to Academy life. As a result of this, we expect that all students bringing a mobile phone to school, hand it in at the start of the day and have it returned to them before leaving.

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 – always install the latest updates
- Securely storing academy devices at all times and not leaving any devices in an unsecure location (e.g. in a car)

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 2.

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 to the ICT Support Provider.

10. How the Academy 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 E-Safety 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Academy 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 and deputy/deputies 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.

12. Monitoring arrangements

All incidents of online safety are logged via the CPOMS system in line with all safeguarding incident logs. The DSL and deputy/deputies monitor all information logged on CPOMS.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Anti-Bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use agreement
- Safer Working Practice in Schools Guidance 2019
- Data Storage and Retention Policy
- Staff Handbook

14. Use of digital and video images - Photographic, Video

The school is responsible for the safe use of photographic and video images of all pupils. When using photographic and video images staff must:

- follow school policies concerning the sharing, distribution and publication of those images. Images should only be taken on school equipment. Personal equipment of staff should not be used for such purposes.

- ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission .
- must ensure pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- ensure that written permission from parents or carers has been obtained before photographs of pupils are published.

15. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.
- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

16. Communications

When using communication technologies the school considers the following as good practice:

- The official school email service (via Google Gmail and Classroom) is regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Only official email addresses should be used to identify members of staff.

17. Inappropriate Use

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

17.1 User Actions:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gaming (educational)
- On-line gaming (non educational)
- On-line gambling
- Use of social networking sites
- Use of video broadcasting e.g. YouTube unless agreed by senior management

18. Remote Learning

During periods of remote education, measures are in place and must be adhered to in order to safeguard pupils and teachers online.

The measures are listed within Appendix 3: Online Learning Guide for Parents.

This guide will be shared with parents and carers and studied by staff prior to the commencement of any online contact with pupils during periods of home learning

Appendix 1: 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 Academy 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 username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it
- I understand that I must be socially responsible with regard to using the internet and other communication technologies, including treating others with respect, and reporting instances of online bullying.
- I agree that all copyright and intellectual property rights must be respected.
- I understand that the irresponsible use of the network and internet will result in the loss of network or Internet access, plus the Academy may instigate additional sanctions. For serious breaches the Academy may involve the police.

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
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it in school time 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 Academy will monitor the websites I visit

Signed (pupil):

Date:

Parent's Consent for Web Publication of Work

I agree that my son/daughter's work may be electronically published.

Parent's Consent for Internet Access

I have read and understood the Academy e-safety rules and give permission for my son / daughter to access the Internet. I understand that the Academy will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

In the absence of any negligence, I understand that the Academy cannot be held responsible for the content of materials accessed through the internet. I agree that the Academy is not liable for any damages arising from use of the internet facilities

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:

The Academy may exercise its right to monitor the use of the Academy's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the Academy's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

All pupils use computer facilities including Internet access as an essential part of learning. Both pupils and their parents/carers are asked to sign to evidence that the e-Safety Rules have been understood and agreed.

HOME ACCESS TO ICT / INTERNET					
Does your child have access to ICT and Internet at home:	Yes		Please specify what device if Yes:	Desktop Computer	
	No			Laptop	
				Tablet / iPad	
				Mobile Phone	
				Other (please specify)	

PARENT / CARER EMAIL ADDRESS(ES)			
If you have an email address please provide it below			
Name		Email Address	
Name		Email Address	

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

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

Name of staff member/governor/volunteer/visitor:

When using the academy's ICT systems and accessing the internet in school, or outside Academy on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the Academy's reputation
- Subscribe or register to any websites without first obtaining approval from the Academy Information Officer/Data Protection Lead to ensure compliance with the necessary procedures
- Access social networking sites or chat rooms for personal use. The Academy uses social media platforms such as Twitter in order to publicise the school. Updates made on behalf of the Academy via our social media platforms must first be approved by a member of the Senior Leadership Team.
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without first checking that the necessary parental consent has been provided
- Take any photographs of pupils using a personal device.
- Share confidential information about the academy, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Post or share any materials on the academy website and social media streams without first checking copyright to ensure there is no breach of copyright laws

I will only use the academy's ICT systems and access the internet in school, or outside Academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the Academy will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the Trust's data protection policy.

I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Staff member signatures are recorded on the Behaviour Watch System

Appendix 3: Online Learning Guide for Parents and Carers

Safeguarding pupils and teachers online

Keeping pupils and staff safe during remote education is essential. Staff delivering remote education online should be aware that the same principles set out in the Staff Handbook will apply.

- Staff shouldn't communicate with parents or pupils outside school channels (for example, they shouldn't talk to parents using their personal Facebook accounts, or contact pupils using their personal email addresses or phone numbers). Staff using a personal phone will always block their number - please be ready to accept withheld numbers, if your child is working at home.
- Safety Online – advice for parents is available and should be sought as necessary. Staff may direct families to resources as they see necessary.
- A useful site for families: <https://www.thinkuknow.co.uk/> There is also a link to report online concerns.
- If parents have any concerns it is important that even though they are accessing remote learning they can still get in touch with school and speak to a child protection officer. Please contact the Vice Principal or your home learning contact if you have any issues you would like to discuss.

Harmful or upsetting content

Staff and parents can get support by:

- reporting harmful online content to the [UK Safer Internet Centre](#)
- getting government advice and trusted resources from [Educate Against Hate](#) on safeguarding from radicalisation, building resilience to extremism, and promoting shared values

Bullying or abuse online

- get advice on reporting online abuse from the National Crime Agency's [Child Exploitation and Online Protection command](#)
- get advice and support from [Anti-Bullying Alliance](#) for children who are being bullied
- online issues should be reported to school and will be logged and dealt with accordingly

Teaching from home – Virtual and live lessons

Teaching from home is very different from teaching in the classroom. Staff will aim to find a quiet or private room or area to talk to pupils, parents or carers. They may be working from home or in the school building.

When broadcasting a lesson or making a recording, they will consider what will be in the background, and where possible will blur the background, so as not to cause distraction or show any identifying features within the household.

- They will dress appropriately and your child should do the same – this means day time clothing which is suitable for meeting others in
- They will not film from a bedroom, and your child should not take part in a lesson from a bedroom (where possible)
- Staff will use professional, appropriate language and will remind pupils to do the same

Staff may record live stream lessons using Google Meet. Parents and students will be asked for verbal consent if the lesson is to be filmed.

We will use CPOMS (a school logging system) to keep a log of who is conducting live streams and when.

We would ask parents to be mindful of what they say and do in the background of any live lesson.

What to Expect

You will be contacted in advance if a teacher plans to offer your child live lessons. This will be a 1-2-1 or 2-2-1 lesson. You will need to provide an email address, to which a link to a live lesson will be sent. You will need to click on the link at the arranged time; the teacher will log in, and the lesson will go live.

Any live lesson contact will be delivered through Google Meet. There is a chat function, which teachers can disable as appropriate.

You are welcome to join in a live lesson to support your child, should you wish and should you and the teacher feel this is conducive to learning – please discuss with the teacher in advance.
