Springwell Leeds

Online Safety Policy

July 2025

Version	5	**Review Cycle**	Annual
Date of Approval	08/07/25	**Approval Level**	Principal

WELLSPRING
We Make A Difference

Introduction 3
Scope of the Policy 3
1. Aims 4
1.1 The 4 Key Categories of Risk 4
2. Legislation and guidance 4
3. Roles and responsibilities 5
3.1 The governing board 5
3.2 The Executive Principal 5
3.3 The designated safeguarding lead (DSL) 5
3.4 The ICT Support Provider 6
3.5 All staff and volunteers 6
3.6 Parents 6
3.7 Visitors and members of the community 6
4. Educating pupils about online safety 7
4.1 Key Stage 1 7
4.2 Key Stage 2 7
4.3 Key Stage 3 7
4.4 Key Stage 4 7
5. Educating parents about online safety 8
6. Cyber-bullying 8
6.1 Definition 8
6.2 Preventing and addressing cyber-bullying 8
7. Acceptable use of the internet in school 10
8. Pupils using mobile devices in school 10
9. Staff using work devices outside school 11
10. How the Academy will respond to issues of misuse 11
11. Training 12
12. Monitoring arrangements 12
13. Links with other policies 12
14. Use of digital and video images - Photographic, Video 13
15. Data Protection 13
16. Communications 13
17. Inappropriate Use 14
17.1 User Actions: 14
18. Remote Learning 14
Appendix 1: Acceptable use agreement (pupils and parents/carers) 16
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) - LINK 18
Appendix 3: Online Learning Guide for Parents/Carers, Students and Staff 19
Appendix 4: Social Media Protocol - Using Academy Social Media Accounts 21
Appendix 5: Staff Agreement – Issue of Mobile ICT equipment 25

Introduction

This policy provides additional information and guidance as to how the provisions made in the Wellspring Academy Trust Online Safety Policy will be applied and implemented at Springwell Leeds Academy and will be updated annually in order to reflect any changes, statutory or otherwise that may be introduced.

Scope of the Policy

New technologies have revolutionized 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 Leeds Academy, 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. Online 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 online 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 online safety behaviour that take place out of school.

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.

1.1 The 4 Key Categories of Risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 Doug Martin

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 (DSL)

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 cyberbullying 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 (Primary ICT) is responsible for technical – Infrastructure, Equipment, Filtering and Monitoring

- Primary ICT will be responsible for ensuring that the Academy's infrastructure and network is as safe and secure as is reasonably possible and that approved policies and procedures are implemented.
- The Designated Safeguarding Lead is responsible for ensuring the filtering put in place is fit for their academy and to implement monitoring of Online activity within their academy.
- There is an expectation that both IT staff and Designated Safeguarding Leads work together closely. This collaboration between the DSL and IT service providers is critical to ensure that systems not only function technically but also align with broader safeguarding strategies.

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

4.1 Key Stage 1

In KS1 , 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

4.2 Key Stage 2

In KS2, pupils 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 the primary stage**, 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

4.3 Key Stage 3

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

4.4 Key Stage 4

Key Stage 4 pupils 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
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant and presented in a manner appropriate to the age and needs of our pupils.

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.

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

6.3 Examining electronic devices

Any member of staff authorised to do so by the Principal on site, 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 Principal or other Senior Leader on site.
- 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 cooperation

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 Principal on site 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 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 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
- The Academy's Behaviour and Relationships 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.

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 1/2). 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, governors and visitors (where relevant) to ensure they comply with the above.

Further information is set out in the acceptable use agreements. Please refer to the Wellspring Academy Trust IT Acceptable Use Policy and Password Policy for the agreement for Staff and Volunteers, and refer to Appendix 1 of this guidance document for the acceptable use agreement for pupils.

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**.

Academy staff will make appropriate arrangements to ensure that pupils' mobile phones are collected and stored safely and securely

In the event that an ICT device is issued for a Pupil to use from home, this will need to be approved by a member of the Senior Leadership Team, and a Parent/Carer ICT Agreement will need to be issued, and signed by parent/carer upon collection/delivery of the device (see Appendix 6)

9. Staff using work devices outside school

Staff members may be allocated a mobile ICT device in order to assist them with their role. The Staff ICT Agreement document must be read and signed for by the staff member upon receipt of the device (see Appendix 5)

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)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates - this requires regular full shut down and restarts of devices and installing updates when prompted
- 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 unless permission for personal use is provided by the Principal
- Seek advice from the ICT Support Provider if they have concerns about the security of a device.
- Any damage/loss must be reported to the appropriate staff member immediately

If staff have any concerns over the security of their device, they must:

- Immediately report the incident to the local managed service provider.
- Notify the Trust using the email security@wellspringacademies.org.uk from a colleagues email address. If this is not possible due to the system being down please notify by telephone or any other means necessary.
- Follow the steps set out in the Cyber Security Incident Management Plan (LINK) whilst completing the incident management report

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).

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 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
- Behaviour and Relationships 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.
- 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.
- Ensure photographs are removed from social media in line with WAT retention policies
- Ensure photographs are stored securely and only stored for the length of time they are required

Pupils must:

- not take, use, share, publish or distribute images of others without their permission

15. Data Protection

Data at Springwell Leeds Academy will be managed and controlled in line with the Wellspring Academy Trust's

- Data Protection Policy
- Data Retention and Disposal Policy

Copies of these documents are available through the Academy website and Staff Intranet.

16. Communications

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

- The official school email service (via Google Gmail and Classroom and Arbor App, Arbor Email and ArborText)) 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/ social media 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
- Stocks and shares
- Use of social networking sites - other than those Academy accounts authorised by senior leaders
- 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, Students and Staff.

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 hand over my phone to staff look after when asked to do so ● 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 online 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 Online 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) - LINK

Appendix 3: Online Learning Guide for Parents/Carers, Students and Staff

Safeguarding Pupils and Staff 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. 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 or to children in their home is very different from teaching in the classroom. Staff will aim to use a quiet space 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, if teaching from 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
- 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 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 lessons 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, 2-2-1 lesson, or a small group 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 member of staff 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.

At times, live lessons are undertaken to re-engage children in learning, or to support children who have been out of education for a period of time. For this reason, the focus may initially be on relationship building and SEMH skills development, before progressing towards academic lessons. A programme of lessons may begin with a short series of checkins, before exploring barriers to attendance, and then adding elements of formal learning.

Appendix 4: Social Media Protocol - Using Academy Social Media Accounts

Social Media Protocol - Academy Social Media Accounts

This protocol applies to all Academy staff, volunteers and temporary staff and references all current and future Academy Social Media platforms, (including but not limited to; YouTube, Facebook, Twitter)

1. **Social Media Posting:**

1.1. Staff with delegated authority to post:

1.1.1 It is important that the good work that happens within the academy is shared and, in order to ensure the necessary controls are in place prior to any information being placed on social media via the Academy accounts, **only designated staff members can post directly from the Academy social media accounts**

1.1.2 the staff members with access to post can be found HERE - only these staff members should hold log-in details

1.1.3. Any requests to share the logins more widely, must be made via the Principal on site to the delegated manager of the Academy Social Media Accounts, who will then send details to the person and add them to the list of authorised users.

1.1.4 It is good practice for all social media posts to be secondary peer checked, although we understand this may not always be possible due to timings of the posts. Staff members with designated access to post vis the Academy Social Media platforms are trusted to use their judgement on this, and, where this is not possible, they must ensure the information being posted is appropriately double checked by them (to ensure it complies with the points contained within 1.2 below).

1.2 GDPR and Social Media - Secondary Peer Checks prior to posting (good practice guide):

1.2.1. When posting anything via social media, it is good practice for a secondary check to be made by a colleague. This is to check for:

- Wording/content check 1 - for any spelling and/or grammar mistakes
- Wording/content check 2 - for any typos and general content check - in case any amendments need to be made
- Photo check 1 - That the identity of all students contained within the photo is known to the uploader so that a check can be made on their current photo consent, which is held in Arbor (please confirm with your site's Office Manager if unsure)
- Photo check 2 - If the photograph contains any students for whom the academy does not hold current photo consent then those students' faces (and any identifiable features) are removed from the photo (usually via photo editor/paint)
- Photo check 3 - That the edited photo is double-checked to make sure that the editing/redacting process has worked before it is uploaded
- Set-up - to ensure, if the ability to view/comment by external parties should be disabled, that this is in place

1.2.2 Prior to the post being uploaded, the uploader must make a final check on the photo and content once it has been successfully uploaded to the social media site to ensure all information is in order as per the checking process

1.3 Procedure prior to posting

1.3.1 Staff member requesting the post forwards content for the post on to a staff member listed with delegated authority to post, confirming;

- Which social media platform should be used
- All names of students within any photo/s that need to be contained within the post
- Accessibility - e.g. does this need to be open to all to view, comments disabled etc.
- They have checked the information contained within the proposed post and are confident all is ok

1.3.2 Appropriate checks on the information are made by the staff member with authority to post

1.3.3 When both parties have confirmed the content is ok to be posted, the post is sent via the appropriate Academy social media platform by the staff member with authority to post

1.3.4 Unless agreed otherwise by a site SLT member, posting via Academy social media platforms that contain photos must only take place during school hours, this is in order to ensure any issues can be rectified quickly if needed

2. Account Information and Login Credentials:

2.1 No staff member should create an Academy social media account on any social media platform

2.2 All Academy social media accounts are managed centrally, and no account is created without the express permission of the Executive Principal

2.3 The Academy social media account information and management of this is held and maintained by the Academy Social Media Manager (this includes any add-ons/apps to assist the management of the accounts)

2.4 All Academy social media accounts are linked to a central email address and not to an individual email address (office@springwellacademyleeds.org)

2.5 Sharing of social media login credentials should only be actioned by the Academy Social Media Manager, who will be responsible for updating this record. Any requests for staff members to be added to this list should be directed to the Academy Social Media Manager

2.6 The delegated manager of the Academy Social Media Accounts is responsible for ensuring the social media account passwords are:

- compliant with GDPR polices
- changed on a regular basis, in line with the password policy
- Changed whenever a staff member with responsibility to post leaves the Academy
- Reshared with all relevant staff members as and when required

3. ‘Likes’, Comments and ‘Re-posts’

3.1 Likes / retweets / comments via the Academy Social Media Accounts can only be made by the staff members that have permission to post.

3.2 Any likes / retweets / comments from personal/individual social media accounts are undertaken without the input of the academy however, staff must be mindful of the corporate image whenever they include their input into anything via social media that could link them to the academy (see the Staff Handbook / Code of Conduct and relevant staff policies and procedures for further information)

4. Reporting and Blocking Inappropriate Content:

4.1 Any content deemed inappropriate must be brought to the attention of the Associate Principal and Executive Principal immediately and measures taken to ensure the content is removed/blocked as soon as possible

4.2 The management / action of this will be undertaken by the delegated manager of the Academy Social Media Accounts under the direction of the Executive Principal/Associate Principal

4.3 A log will be held and maintained by the manager of the academy social media accounts of any issues / blocked posts / inappropriate comments etc

4.4 The manager of the academy social media accounts will be responsible for undertaking regular checks of all social media posts to ensure any negative comments are seen and addressed promptly, and also responsible for keeping a log of engagement to be reported back as appropriate

5. Social Media Platforms and intended use

5.1 There are a number of current social media platforms and we are aware that online platforms are being developed all the time. In order to ensure we are using the current platforms in a consistent manner, the following guide needs to be referred to:

5.1.2 Facebook

- Audience - Parents/Carers/Community
- Used for - Advertising job vacancies, communicating with parents and carers around generic information (e.g. Newsletter, general school information), advertising school events to the community (e.g. job fairs, community and charity events)
- Posts - ability to comment to be removed prior to posting, ability to ‘like’ to be enabled

5.1.3 BlueSky (Twitter / “X” is no longer to be used)

- Audience - Trust colleagues and schools, stakeholders
- Used for - promoting the good work happening in the schools (photos, short/sharp content), and advertising job vacancies
- Posts - ability to retweet and comment generally enabled

5.1.4 Youtube

- Audience - across the web, although can be restricted for specific posts where necessary

- Used for - sharing specific videos with a specific group, and/or sharing videos with all for promotional purposes
- Posts - to be limited to a specific group where appropriate (e.g. if sharing with a group of parents/carers - e.g. Y11 leaver video), can also be used to share with a wider audience e.g. good practice/training video clips. Access rights to be adapted where appropriate depending on the post content. Ability to comment to be removed prior to posting, where appropriate
- Due to the way in which Youtube accounts are set up, only the Manager of the Academy Social Media Accounts can post on the Academy Youtube channel. Any requests for posts to be added need to be forwarded on to the Academy Social Media Manager by a staff member with delegated authority to post (see list)

6. Personal Social Media Accounts:

6.1 Please refer to the Staff Handbook, Code of Conduct and relevant Policies regarding use of personal social media accounts. This includes but is not limited to the Disciplinary, ICT and Safeguarding Policies and Procedures

6.2 All staff must be mindful of the need for professionalism when using social media platforms both inside and outside of work and also be mindful that any breach of policies and procedures regarding staff conduct could result in disciplinary procedures.

6.3 Social media is a useful tool when used in the correct manner and positive use of social media is encouraged - e.g. to share job vacancies to a wide audience of professionals

Appendix 5: Staff Agreement – Issue of Mobile ICT equipment

Device assigned: **iPad / Laptop / Mobile Phone / Chrome book**

Serial No: …….

Date Issued: …….

Issued By: …….

Issued To: …….

For (area): …….

- ICT devices remain the property of Springwell Leeds Academy and are intended to aid Springwell Employees in their role.
- The member of staff that the ICT device has been allocated to must take full responsibility for its proper use, in line with Academy e-safety and data protection policies.
- Devices must be stored securely, and locked away when not in use
- All Photos that are taken using the ICT device assigned must be transferred across to a secure Academy file location as soon as practicably possible
- No photos should be left on ipads, (as these are not GDPR compliant)
- In the event that employment with Springwell Academy ceases, all ICT equipment must be returned to the Admin Manager on site, and must not be transferred directly on to a colleague
- In the event that you start work at another establishment within the Wellspring Academy Trust, the device must be returned to the site it was issued from and must not be taken with you to another site.
- In the event that any device that you are responsible for is lost or damaged, this must be reported to the appropriate staff member immediately.
- Any damages or loss of ICT equipment that is deemed by the Principal to have been caused as a result of improper use or negligence by the member of staff who is responsible for the device may incur a charge to the member of staff. The charge will be in line with the cost of a replacement device
- If the device that you are signing for is intended to be used by other members of staff (i.e. iPads that are shared and used flexibly), you must ensure that the above expectations are shared with any staff that will use the device, and a regular check of the equipment must take place by yourself

I confirm that I have read this agreement and I understand my responsibilities:

Signed: …….

Print Name: …….

Date: …….

Appendix 6: ICT Parent/Carer Agreement

Device assigned: …….

Serial No: …….

Date Issued: …….

Student Name: …….

- I understand that the ICT device (as stated above) is loaned to me for my child's use for the following period: ……. to ……. , following which time I must return the device to Springwell Leeds Academy.
- The device, as stated above, remains at all times the sole property of Springwell Leeds Academy.
- I take full responsibility for the device's proper use, in line with the Academy Online Safety Acceptable Use Policy, and, as previously agreed by me within the Academy admissions paperwork.
- I understand that the device is being loaned in order to assist my child in completing work that is sent home from the school during the self-isolation period.
- In the event that the device is lost or damaged, I will report this to the school immediately.
- In the event of loss/damage, I understand that damage procedures will be followed which may result in a bill being issued to me if the loss/damage is deemed to have been caused as a result of improper use or negligence.
- I understand that in the event of loss/damage, the Academy will be unable to provide my child with a replacement device.
- Springwell Leeds Academy has loaned the ICT device as stated above to your child in order to help support them during the period of extended self-isolation. Access may be withdrawn if used irresponsibly. We encourage students to make use of the device for their benefit and to use it safely and responsibly.

Parent/Carer Signature:

I confirm that I have read this agreement and I understand my responsibilities and expectations.

Signed: …….

Print Name: …….

Date: …….

Appendix 7: Springwell Leeds Academy Protocol - iPads

Standard iPad set up:

CLASS iPads

Set up - STAFF use only

Standard App List

1. Camera/Gallery
2. Tapestry
3. Immersive Interactive
4. Kahoot!

Points:

- Each Teacher/Class Lead is allocated a Class ipad.
- Responsibilities around ipads sit with the class teacher/lead (in line with the ICT agreement and Online Policy)
- Class ipads are used by Staff only (Chrome books are available for use in lessons, if needed)
- Photos are transferred on to the relevant platform asap (e.g. Tapestry, Google Drive) - no photos should remain stored on the device at all
- Any additional App requests must be submitted to the SLT member below, who will update the standard issue list, if agreed and rolled out

EAST	SOUTH	NORTH
Mark Bainbridge	Ashley Knapton-Smith	John Gillard

Exceptions to the standard issue:

We are aware that, for specific subjects, there may be exceptions to this (e.g. Maths, Music) and, in these circumstances, the Specialist Teacher may require additional Apps in line with their subject

In these circumstances, the ipad/ipads will be issued to the Specialist Teacher, and must be:

- Clearly labelled with the appropriate label (e.g. Music / Maths)
- If these need to be used by students (for the purpose of specialist lessons), they must also be clearly labelled as ‘Student Use’

It is the Specialist Teacher’s responsibility to ensure compliance with the necessary procedures around the use of these ipads, and the same rules apply around ensuring photos are not stored on the devices, and around requesting any additional apps via the relevant SLT member on site