Aspire Schools
E-Safety and Acceptable Use Policy

Policy adopted:	September 2026
Policy reviewed by:	Executive Team, Trustees To be ratified by Trustees: Autumn 2026
Updates from last version	General updates throughout with minor date and name changes Addition of section 13 – Use of Ai Additions to device loan form
Review date:	July 2027

Contents

1. Purpose and context 3
2. Legislation and guidance 3
3. Roles and responsibilities 3
3.1 The Board of Trustees 3
3.2 The Headteacher 4
3.3 The Designated Safeguarding Lead 4
3.4 The ICT Manager and ICT Support Company (Turn IT On) 4
3.5 All staff and volunteers 5
3.6 Parents/Carers 5
3.7 Visitors and members of the community 5
4. Educating students about online safety 5
5. Educating parents about online safety 6
6. Cyber-bullying 6
6.1 Definition 6
6.2 Preventing and addressing cyber-bullying 6
6.3 Examining electronic devices 7
7. Acceptable use of the internet in school 8
8. Managing internet access 8
9. Students using mobile devices in school 8
10. Staff using work devices outside school 9
11. Staff Work Mobile Phones 9
12. E-mail 9
12.1 Email Protection 9
13. Use of AI 10
14. Social networking 111
15. How the school will respond to issues of misuse 133
16. Monitoring arrangements 13
Appendix 1 - ICT Acceptable Use Policy for Students 14
Appendix 2 - Staff, Trustee and Visitor Acceptable User Agreement / Code of Conduct 15
Appendix 3 – Aspire Schools device loan agreements for Staff 177

1. Purpose and context

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, 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 seminudes and/or pornography), sharing other explicit images and online bullying
- **Commerce –** risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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 headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Board of Trustees

The Board of Trustees has overall responsibility for monitoring this policy and holding the CEO to account for its implementation.

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

All trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Leads (DSLs) and Deputy DSLs are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher Heads of School/AMP Leads, IT Manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's Anti-Bullying and Behaviour Regulation and Relationships policies
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and Board of Trustees.

This list is not intended to be exhaustive.

3.4 The ICT Manager and ICT Support Company (Turn IT On)

The ICT Manager and provider is responsible for:

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

3.5 All staff and volunteers

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

- Reading, understanding and complying with this policy
- During new staff induction and September Inset days, staff will indicate that they have read and understood this Policy and that its contents will be complied with
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that students follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents are expected to:

- Notify a member of staff or their respective Head of School/Provision 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 resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating students about online safety

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

All schools have to teach relationships and sex education and health education in secondary schools

Students will be taught to:

- Use technology safely, respectfully and responsibly
- Identify AI risks and benefits.

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of school, students 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

The safe use of social media and the internet will also be covered in other subjects where relevant.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

5. Educating parents about online safety

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

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their respective Head of School/Provision and/or the DSL.

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 school Behaviour Regulation and Relationships Policy)

6.2 Preventing and addressing cyber-bullying

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

Aspire Schools will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school also sends information/leaflets 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 school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

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

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' 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 school rules

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

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

**Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.*

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

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

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

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and trustees 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.

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

8. Managing internet access

Students will have supervised access to Internet resources

- Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the students as these can return undesirable links.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.
- Our internet access is controlled through the local authority web filtering service. Our Antivirus also filters internet access to give us an extra layer of protection.
- Smoothwall: this service monitors all activity on Student/Staff IT devices. Staff and students are aware that all computer and laptop activity is monitored. Smoothwall uses software to detect any threats in any language/Images. If intervention is required, the incident is escalated to the school's DSLs.

- *A screen shot captures the incident*
- *The user ID, machine name, time, date and IP address are recorded*
- *Behaviour Analysts review the incident to determine if it requires intervention (or not)*
- *Illegal and life-threatening incidents will be reported to the site DSL immediately, by phone*
- *Incidents that require intervention are documented in an encrypted report that's emailed to the school's nominated contacts.*
- *Weekly and Monthly Reports are sent to the DSL's outlining the different type of incidents that Smoothwall has captured during that period. This can be useful to spot trends.*

- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to a member of SLT.
- It is the responsibility of the school, by delegation to the IT manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

9. Students using mobile devices in school

Students are not permitted to use them during Lessons. All Phones need handing in at the start of the school day.

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1). Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behavior policy, which may result in the confiscation of their device.

10. Staff using work devices outside school

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

- Keeping the device password-protected – 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
- 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

Staff members must not use the device in any way which 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 the IT Manager or external IT provider Turn IT On.

11. Staff Work Mobile Phones

Mobile Phones are issued based on job role and school need. These devices remain the property of the company and must be returned upon termination or role change. Aspire Schools reserves the right to monitor usage of work mobile devices and data may be accessed for compliance and security purposes. Devices must be protected with a secure password, PIN, or biometric authentication. Employees must report lost or stolen devices immediately to the IT Manager.

12. E-mail

The use of email within school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or student based, within school, between schools or international.

- The school gives staff their own email account, to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact students or parents using personal email addresses.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- All students must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone.
- Staff must inform a member of SLT if they receive an offensive e-mail.

12.1 Email Protection

Microsoft 365 is used for all of our emails. Microsoft 365 email is encrypted using Transport Layer Security (TLS). This is a protocol that securely encrypts and delivers inbound and outbound mail while disabling

eavesdropping between mail servers. Multi factor authentication is applied to all Staff O365 accounts when accessing Cloud Data (Outlook/Teams/Onedrive) this adds further protection to our Emails and Data. Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs.

Therefore, Aspire Schools requires all staff to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the IT Manager regarding any suspicious emails.

13. Use of AI

Artificial Intelligence (AI) refers to computer systems that can perform tasks normally requiring human intelligence, including:

- Generating text
- Creating images
- Producing audio or video
- Analysing information
- Summarising documents
- Answering questions
- Supporting planning and administrative tasks

Examples may include:

- Microsoft Copilot
- ChatGPT
- Google Gemini

Aspire Schools will ensure that any use of AI is:

- **Safe**
  AI must not expose children to harm, inappropriate content or safeguarding risks
- **Ethical**
  AI must be used honestly and transparently
- **Secure**
  Personal and confidential information must be protected
- **Inclusive**
  AI should support accessibility and equal opportunity
- **Educational**
  AI should enhance learning rather than replace critical thinking

Staff may use approved AI tools for:

- Lesson planning
- Resource creation
- Administrative support
- Drafting communications
- Generating ideas and examples
- Creating differentiated learning materials
- Supporting accessibility requirements

Staff must:

- Check all AI-generated content for accuracy
- Verify information before sharing with students
- Exercise professional judgement
- Follow copyright and intellectual property requirements
- Ensure AI-generated content is appropriate for the age and needs of students

Staff must not:

- Upload confidential student information into public AI systems
- Upload safeguarding records
- Upload SEND records containing identifiable information
- Upload personnel files
- Share passwords or access credentials
- Allow AI systems to make safeguarding decisions
- Rely entirely on AI-generated content without review

AI must never replace professional judgement.

Students may use AI tools when authorised by a member of staff and where educationally appropriate. Permitted uses may include:

- Research support
- Revision activities
- Generating ideas
- Language support
- Draft planning
- Coding assistance

Students must:

- Acknowledge when AI has been used
- Verify information from trusted sources
- Follow teacher instructions
- Use school-approved systems where available

The school recognises that AI may present safeguarding risks, including:

- Deepfake images and videos
- AI-generated bullying or harassment
- Inappropriate content
- Misinformation
- Online grooming risks
- Creation or sharing of harmful images

Any safeguarding concerns involving AI must be reported immediately to the Designated Safeguarding Lead (DSL).

14. Social networking

We block/filter access for students to social networking sites.

Safeguarding students is a key responsibility of all staff, and it is essential that everyone within Aspire Schools considers this and acts responsibly if they are using social networking sites out of working hours.

Anyone working in Aspire Schools either as a paid employee or volunteer must not communicate with students supported by Aspire Schools' services via social networking.

To further safeguard and protect students and staff.

The following are **not considered acceptable** within Aspire Schools:

The use of the Trust's or individual school's names, logos, or any other published material without written prior permission from the CEO. This applies to any published material including the internet or written documentation.

- The posting of any communication or images which links Aspire Schools to any form of illegal conduct, or which may damage the reputation of Aspire Schools. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of Aspire Schools.
- The posting of any images of employees, students, or anyone directly connected with Aspire Schools whilst engaged in school activities.

In addition to the above everyone within Aspire Schools must ensure that they:

- Have set their security settings on their personal profile at the highest possible settings so that no content of their profile may be viewed by any party not previously agreed as a 'friend'.
- Do not use computer equipment provided for their professional use by Aspire Schools for accessing Social Networking Sites either at work or at home. Any access to Social Networking Sites must therefore only take place using privately owned computers
- Do not make any derogatory, defamatory, rude, threatening, or inappropriate comments about Aspire Schools or anyone at or connected with Aspire Schools.
- Using social networking sites irresponsibly and allowing their personal/professional reputation, nor Aspire Schools' reputation to be compromised by inappropriate postings.
- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

Everyone within the Aspire Schools trust and its services must not accept the following as 'friends' on such sites unless they are members of their immediate family:

- Any student accessing any of Aspire Schools' services
- Any past student who accessed any of Aspire Schools' services who is under the age of 18 years
- Any parent/carer of a student who is accessing any of Aspire Schools' services

If any such people are already 'friends' they should be removed immediately.

Responsibility for adhering to these restrictions lies solely with the individual user. Any use of Social Networking that is deemed inappropriate by the management of Aspire Schools will be reported to the management committee and will be dealt with in line with the Aspire Schools Staff Disciplinary Policy.

15. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour and E-Safety and Acceptable Use policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

16. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS (**CPOMS** is the market leading software solution for monitoring Safeguarding, wellbeing, and all pastoral issues)

This policy will be reviewed every year by the IT Manager. At every review, the policy will be shared with the Board of Trustees. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve, and change rapidly.

Appendix 1 - ICT Acceptable Use Policy for Students

Agreement / E-Safety Rules

- I will take care when using the school IT equipment and use it properly
- I will only share my username and password with trusted adults
- I will hand my phone in at the beginning of the school day
- I will tell an adult if I see anything that upsets me
- I will make sure that when I blog, I am responsible, polite, and sensible
- I will use a safe name and not my real name on the internet
- I know I am only allowed to go on the internet if my teacher has given me permission
- I will only take a photograph or video of someone if they say it is alright
- Any messages I send will be polite
- I will not deliberately write anything which upsets other people
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment
- I understand that if I do not follow these rules, I may not be allowed to use the school computer or internet for a while, even if it was done outside school

Parent/ Carer signature

We have discussed this and ……. (child's name)

agrees to follow the e-Safety rules and to support the safe use of ICT at Aspire Schools

Parent / Carer Name (PRINT) ……..

Parent / Carer (Signature) ……..

Date……

Appendix 2 - Staff, Trustee and Visitor Acceptable User Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff must sign this agreement and adhere to its contents.

Any concerns or clarification should be discussed with a member of SLT.

- I will only use the school's email / Internet / MS Teams and any related technologies for professional purposes or for uses deemed 'reasonable' by the CEO or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will only use the approved, secure email system(s) for any school business.
- I will not email documents giving details of students unless on a secure system such as Egress.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the CEO or Governing Body.
- The use of USB sticks is forbidden. If one is required, this has to be authorised by the CEO or Governing Body.
- Software cannot be installed without an admin password. Should a software package be needed, installation of this can be requested from the IT Manager via the Ticketing System.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken with school devices, stored, and used for professional purposes in line with school policy and with written consent of the parent, carer, or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or head teacher. I understand I cannot use my mobile phone to take photos of children
- I understand that all my use of the Internet and other related technologies can be monitored and logged into and can be made available, on request by the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.

Staff must not:

- Upload confidential student information into public AI systems
- Upload safeguarding records into public AI systems
- Upload SEND records containing identifiable information into public AI systems
- Upload personnel files into public AI systems
- Share passwords or access credentials into public AI systems
- Allow AI systems to make safeguarding decisions
- Rely entirely on AI-generated content without review

By signing below, I confirm agreement to follow this code of conduct and to support the safe use of ICT throughout Aspire Schools and its services.

Full Name ……..

Position …… Site …….

Signature …….. Date ……

Appendix 3 – Aspire Schools device loan agreements for Staff

1. This agreement is between:

1) [Aspire Schools] ("the Trust")

2) ("the employee" and "I")

And governs the use and care of devices assigned to individual staff members. This agreement covers the period from the date the device is issued through to the return date of the device to the Trust.

All issued equipment shall remain the sole property of the Trust and is governed by the Trust's policies.

1. The Trust is lending the employee a laptop/desktop (sometimes with mouse/keyboard/webcam/headset) for the purpose of working on site, working from home, working on special projects, hot desking etc.
2. This agreement sets the conditions for the employee taking the equipment home.

I confirm that I have read the terms and conditions set out in the Aspire Schools E-Safety and Acceptable Use Policy and my signature below confirms that I have read and agree to these terms.

2. Damage/loss

By signing, I agree to take full responsibility for the equipment issued to me and I have read or heard this agreement read aloud and understand the conditions of the agreement.

- I understand that I am always responsible for the equipment whether on the Trust's property or not.
- If the equipment is damaged, lost or stolen, I will immediately inform the IT Manager and I acknowledge that I am responsible for full replacement costs.
- If the equipment is stolen, I will immediately inform the police.
- I agree to keep the equipment in good condition and to return it to the Trust on demand from the Trust in the same condition.
- I will not leave the equipment unsupervised in unsecured areas.

- If you have an insurance policy which covers damage, loss or theft of the equipment, please provide the details below. If not, disregards this section.

Insurance provider:
Policy number:
Type of cover:

3. Unacceptable use

I am aware that the Trust monitors my activity on the equipment. I will not carry out any activity that constitutes 'unacceptable use.'

This includes, but is not limited to:

- The laptop you have been provided by the Trust must be used for professional purposes only
- You should not allow any other staff or students access to your laptop
- Laptops should not be left in your vehicle over night or in your vehicle during the day if you are not also in the vehicle

- If you are leaving your laptop alone, you must lock it (WIN KEY + L)
- You must never connect your laptop to public Wifi Networks such as a coffee shop's free wifi.
- You must not use your laptop abroad without permission from the CFOO and ICT Manager. Connecting to Microsoft Apps (Outlook, Teams etc) outside the UK is blocked.

I accept that if I engage in any activity that constitutes 'unacceptable use,' I may face disciplinary action in line with the Aspire Schools Staff Code of Conduct and Staff Disciplinary procedures.

4. Professional use

I will only use this device for professional use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment 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)
- Make sure the equipment locks if left inactive for a period
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact the IT Manager on the email dcocking@aspireschools.org.uk or log a ticket with Turn IT On.

6. Return date

I will return the device in its original condition to the IT Manager within 5 days of being requested to do so. I will return the equipment to the Trust upon resignation, dismissal or if I leave the employment of the Trust for any other reason.

By signing below, when I have been given either a phone or laptop/desktop/accessories as part of my role within Aspire Schools, I confirm that I have read and agree to the rules and conditions within 'Appendix 3 – Aspire Schools device loan agreements for Staff' of the Aspire Schools E-Safety and Acceptable Use Policy.

Full Name ……..

Position …… Site …….

Device(s) received……..

Signature …….. Date ……