



# Aston Rowant C+E Primary School

## Online Safety and Internet Usage Policy

### Mission Statement

**Vision:** To be a community of courageous life-long learners, who are rooted in God, live out our Christian values and enjoy life in all its fullness. *(Col 2:1-7)*

**Mission:** Growing together, rooted in God and inspiring one another through our values and our broad enriched curriculum.

**Strapline:** Growing together, rooted in God, having fullness of life *(Col 2:1-7)*

**Date of Policy: November 2025**

**Date of Policy review: November 2027**

Head Teacher: Mrs H France

Date: 3<sup>rd</sup> November 2025

Chair of Governors: Mr T Sowerby

Date: 3<sup>rd</sup> November 2025

### 1. Introduction

Aston Rowant C+E Primary School recognises that online safety is an essential aspect of safeguarding. This policy combines the school's Online Safety, E-Safety, and Internet Usage approaches into one coherent, statutory-compliant document.

This policy is fully aligned with:

- Keeping Children Safe in Education (KCSIE) 2023, 2024, 2025
- Working Together to Safeguard Children 2023
- Prevent Duty
- UK GDPR & Data Protection Act 2018
- DfE Filtering & Monitoring Standards 2023

It sits alongside:

- Safeguarding & Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Acceptable Use Policies (AUPs)
- Staff Code of Conduct
- Mobile Phone Policy
- Data Protection Policy

### 2. Aims

This policy aims to ensure:

- Safe, responsible and effective use of technology
- Clear processes for responding to online concerns
- Robust filtering and monitoring
- Age-appropriate digital literacy and resilience
- Training for staff, governors and pupils
- Secure data handling and cyber security
- Clear safeguarding escalation routes

### 3. Roles & Responsibilities

#### 3.1 Designated Safeguarding Lead (DSL)

The DSL leads online safety and filtering/monitoring oversight.

**DSL:** Mrs Helen France – **01844 351671**

Responsibilities include (as required in KCSIE):

- Managing online safety incidents
- Responding to filtering/monitoring alerts
- Liaising with TurnItOn (IT provider)
- Reviewing online safety risks
- Ensuring staff training

#### 3.2 Deputy DSL

Supports DSL.

**DDSL:** Mrs Alexi Olsen - **01844 351671**

#### 3.3 Safeguarding Governor

Oversight of online safety, filtering and monitoring.

**Safeguarding Governor:** Rev Jacky Barr - **01844 351671**

#### 3.4 IT Provider (TurnItOn)

**Consultant:** Nigel Lobo

- Provides technical filtering and monitoring
- Updates and maintains systems
- Reports concerns to DSL

#### 3.5 All Staff

All staff must:

- Read KCSIE Part 1 annually
- Report concerns immediately
- Record concerns on **MyConcern**
- Follow Acceptable Use Agreements
- Model safe digital behaviour

### 4. Filtering and Monitoring (KCSIE 2023–2025 Compliant)

#### 4.1 Filtering

Filtering is provided through **TurnItOn** and blocks:

- Harmful content
- Radicalisation/extremist material
- Sexual & abusive material
- Misinformation/disinformation/conspiracy content (*KCSIE 2025 requirement*)
- Online exploitation and grooming behaviour

Filtering is reviewed at least annually.

**GRATITUDE      RESILIENCE      OUTREACH      WONDER      TRUST      HARMONY**

*Growing together, rooted in God, enjoying fullness of life. (Colossians 2:1-7)*

## 4.2 Monitoring

Monitoring systems alert staff to:

- Concerning search terms
- Attempts to bypass filters
- Unsafe digital behaviour
- RSHE-related curiosity spikes that may trigger filters (*KCSIE 2023 guidance for planning*)
- Repeated patterns that indicate risk

## 4.3 Staff responsibilities

Staff must:

- Report any concern immediately to the DSL
- Log incidents on **MyConcern**
- Report technical faults to the office (TurnItOn)
- Never attempt to bypass filtering

## 4.4 Reviewing effectiveness

Filtering and monitoring are formally reviewed:

- Annually
- After safeguarding incidents
- When KCSIE updates (2023–2025)
- At governor visits
- With TurnItOn

---

## 5. Curriculum & Teaching Online Safety

Aston Rowant teaches online safety through:

- Computing curriculum
- PSHE and RSHE
- Assemblies
- Project work
- Guided digital use
- Christian values underpinning safety and respect

Pupils are taught:

- Safe search practices
- Digital resilience
- Recognising unsafe content
- How to report concerns
- How to respond to cyberbullying
- Understanding misinformation and disinformation

**GRATITUDE    RESILIENCE    OUTREACH    WONDER    TRUST    HARMONY**

*Growing together, rooted in God, enjoying fullness of life. (Colossians 2:1-7)*

## 6. Staff Training

In line with KCSIE (annual updates required):

- All staff receive annual online safety training
- DSL receives advanced training
- Staff receive regular updates in briefings
- Staff sign Acceptable Use Agreements
- Staff understand filtering/monitoring responsibilities

## 7. Reporting Online Safety Concerns

Staff must:

1. Act immediately
2. Inform DSL/DDSL verbally
3. Record the concern on MyConcern
4. Use hard-copy forms if MyConcern is unavailable
5. Never investigate - pass to DSL

### Emergency Safeguarding Contacts

- **MASH:** 0345 050 7666
- **Emergency Duty Team:** 0800 833 408
- **LADO (Jo Lloyd):** 01865 810603 / lado.safeguardingchildren@oxfordshire.gov.uk
- **NSPCC:** 0808 800 5000
- **Police (immediate danger): 999**

## 8. SEND, Vulnerability & Inclusion

Children with SEND may have increased vulnerability online.

The school ensures:

- Tailored teaching
- Individual risk assessments
- Additional adult support
- Reasonable adjustments

## 9. Internet Use in School

- Internet use is supervised
- Pupils follow age-appropriate AUPs
- Internet access includes filtering
- Staff guide pupils in safe searches
- Research skills (accuracy, reliability, evaluating content) are taught

**GRATITUDE    RESILIENCE    OUTREACH    WONDER    TRUST    HARMONY**

*Growing together, rooted in God, enjoying fullness of life. (Colossians 2:1-7)*

## **10. Email, Teams & Online Communication**

- Pupils use school-approved accounts only
- Offensive messages must be reported
- No personal data must be shared
- Staff use only school accounts
- Class/Group email accounts preferred
- Teams accounts include safeguarding controls

## **11. Social Networking**

- Access is blocked in school
- Children taught not to share personal details
- Children advised that most platforms require age 13
- Security settings taught
- Parents informed regularly

## **12. Mobile Phones & Emerging Technologies**

- Mobile phones cannot be used during learning time
- Abusive messaging (including sexting) is prohibited
- All technology assessed for risk before use

## **13. School Website & Published Content**

- No personal staff/pupil information published
- Headteacher/editor oversees website content

## **14. Information Security, Data Protection & Cyber Security**

- Data handled per UK GDPR
- Virus protection and updates regularly applied
- Strong passwords required
- Devices kept secure
- Staff understand cyber risks (per KCSIE 2025)

## **15. Risk Assessment, Monitoring & Review**

The school monitors:

- Incident logs (MyConcern)
- Filtering logs
- Network activity
- Review meetings between DSL and IT provider
- ESAT audit frameworks

**GRATITUDE    RESILIENCE    OUTREACH    WONDER    TRUST    HARMONY**

*Growing together, rooted in God, enjoying fullness of life. (Colossians 2:1-7)*

Risks are minimised but cannot be eliminated; pupils are therefore taught resilience and safe practice.

## **16. Handling Online Safety Complaints**

- Pupils → DSL
- Staff misuse → Headteacher
- CP concerns → Safeguarding procedures
- All incidents logged and reviewed

## **17. Communication of Policy**

### **Pupils:**

- Taught E-Safety rules
- Rules displayed in all classrooms
- AUPs signed (KS1/KS2)

### **Staff:**

- Receive full training
- Sign Staff AUPs
- Informed that all internet use can be monitored

### **Parents:**

- AUPs shared
- Updates in newsletters
- Policy on website

## E safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the E safety basics are in place.

Has the school an E-safety Policy that complies with CYPD guidance?	Yes
Date of latest update:	2025
The Policy was agreed by governors on:	Autumn 2025
The Policy is available for staff at:	Document on staff intranet files School website Staffroom safeguarding
And for parents at:	School website
The designated Child Protection Teacher/Officer is	Helen France
The E-safety Coordinator is:	Andy Manning
The E safety Governor is:	Tom Sowerby
Has E-safety training been provided for both pupils and staff?	Yes – each term Also see email etiquette guidance
Do all staff sign an ICT Code of Conduct on appointment?	Yes and Governors
Do children sign an agreement about responsible IT use? Are parents sent a copy of that?	Yes from Years 3-6
Have school E safety rules been set for pupils?	Yes
Are these rules displayed in all rooms with computers?	Yes
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access	Yes
Has the school filtering policy been approved by the SLT?	Yes - annual review
Is personal data collected, stored and used according to the principles of the Data Protection Act 2018?	Yes

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Broadband monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- E safety co ordinator in school and the E safety governor will meet regularly to review monitoring

## Appendices

### **Appendix A - Staff and Governor Acceptable Use Agreement**

To ensure that all staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct.

#### **I. Aims & Background**

This ICT user agreement covers the use of all digital technologies while in school: ie email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school or Local Authority, or other information or systems processors.

This ICT user agreement also covers school issued equipment when used outside of school, use of online systems provided by the school such as VPN or webmail, or other systems providers when accessed from outside school.

This ICT user agreement also covers posts made on any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring staff members or governors professional status into disrepute.

The school regularly reviews and updates with the assistance of the DPO, all user agreement documents to ensure that they are consistent with current school policies as listed at the end of the agreement.

#### **2. User Requirements**

School employees, governors, and third party staff using school systems must comply with the requirements below. Failure to do so could possibly mean disciplinary procedures.

Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may be subject to monitoring.

- a) I will only use the school's ICT resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body in the line of my employment.
- b) I will set strong passwords, following advice provided by the school. I will change it frequently. c) I will not reveal my password(s) to anyone.
- d) I will not use anyone else's password if they reveal it to me and will advise them to change it.
- e) I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or other authority or processing system.
- f) I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols, and retention policy.
- g) I will not engage in any online activity that may compromise my professional responsibilities.
- h) I will only use the schools approved email system(s) for any school business.
- i) I will only use the approved method/s of communicating with pupils or parents and will only communicate with them in a professional manner and on appropriate school business.
- j) I will not support or promote extremist organisations, messages or individuals.
- k) I will not give a voice or opportunity to extremist visitors with extremist views.
- l) I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

- m) I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Head.
- n) I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed. I will seek advice from the School Office.
- o) I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- p) I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other malware systems.
- q) I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- r) I will follow the school's policy on use of mobile phones/devices at school
- s) I will only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
- t) I will only I take or publish images of staff and students with their permission and in accordance the school's consent guidelines. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.
- u) I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.
- v) I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role, and will create a distinction between the two.
- w) I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- x) I agree and accept that any computer or laptop or memory stick loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- y) I will only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.
- z) I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
  - aa) I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
  - bb) I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.

- cc) I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead. dd) I understand that all internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.
- ee) I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- ff) I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
- gg) I will embed the school's online safety / digital literacy / counter extremism curriculum into my teaching.

**3. Links with Other Policies**

I understand that this user agreement is linked to the schools:

- Online and E-Safety Policy
- Email Security and Etiquette Guidance
- GDPR/Data Protection Policy
- Document Retention Policy  Breach Management Policy
- Asset Management Recording Policy
- Disaster Recovery/Business Continuity Planning and Risk Register.
- Safeguarding and Child Protection Policy

**4. Agreement Form**

**User Signature**

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible ICT user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name ..... (printed)

Job title / Role .....

## Appendix B

### Acceptable Use Agreement for KS1

- I will only use the internet or computer when a teacher or adult is with me
- I will only use my own login and password and I will not tell anyone else what it is
- I will not look at or delete other people's files
- I will not bring in memory sticks from home without permission
- If I see anything that upsets me, I will tell an adult
- I will not give out any details about me – like my name or address
- I know school will check my computer and be able to see what I am doing and what sites I have visited
- If I break these rules I know I may be stopped from using the internet and/or computers

### Acceptable Use Agreement for KS2

- I will use the school computers and technology sensibly
- I will ask permission from an adult before I look at the internet
- I will only log on using my own username and password which I will keep confidential
- I will only look at my own work and not delete anyone else's files
- I will not bring in a USBs from home without permission
- I will only email people I know
- I will always be polite and use appropriate language when emailing or sending messages on the computer
- I will not give out my personal information or arrange to meet anyone
- If I think anything on the internet upsets me or a stranger sends me a message, I will tell an adult
- I know school will check my computer and be able to see what I am doing and what sites I have visited
- If I break these rules I know I may be stopped from using the internet and/or computers

## **Appendix C - Letter sent home to all pupils and their parents of KS2. KS1 will have same letter but with their Acceptable Use Agreement**

Dear Parents

In school we have access to the internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. At St James we are aware that young people should have an entitlement to safe internet access at all times. However, school and parents have a duty of care to protect children and ensure that internet use is responsible and safe.

We strongly recommend that children do not use social network sites such as Facebook, Instagram, Snapchat or have YouTube accounts at home. These carry an age-restriction of 13 years old and pose a risk to children. Social networks have no place in our school and so school staff should not be approached by pupils or parents online or invited to join.

Your child has read the following **Acceptable Use Agreement** in class with their teacher. Once they have fully understood them all, your child has signed their name to agree to stick by them. Please read them again at home with your child to show your support of the school in this important aspect of our work. Thank you.

- I will use the school computers and technology sensibly
- I will ask permission from an adult before I look at the internet
- I will only log on using my own username and password which I will keep confidential
- I will only look at my own work and not delete anyone else's files
- I will not bring in a USBs from home without permission
- I will only email people I know
- I will always be polite and use appropriate language when emailing or sending messages on the computer
- I will not give out my personal information or arrange to meet anyone
- If I think anything on the internet upsets me or a stranger sends me a message, I will tell an adult
- I know school will check my computer and be able to see what I am doing and what sites I have visited
- If I break these rules I know I may be stopped from using the internet and/or computers

## Appendix D

### Use of Communication and Information Technology In School

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	*							*
Use of mobile phones in lessons				*				*
Use of mobile phones in social time	*							*
Taking photos on mobile phones				*				*
Use of school hand held devices eg iPads	*						*	
Use of personal email addresses in school, or on school network	*							*
Use of chat rooms/facilities				*		*		
Use of instant messaging				*		*		
Use of social networking sites				*				*

**GRATITUDE RESILIENCE OUTREACH WONDER TRUST HARMONY**

*Growing together, rooted in God, enjoying fullness of life. (Colossians 2:1-7)*

Use of blogs				*		*		
Use of secure learning platforms to collaborate	*				*			

When using email the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email or electronic message 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 parents must be professional in tone and content
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Device loan agreement for pupils

### 1. This agreement is between:

- 1) Aston Rowant Primary School Governing Body (“the school”)
- 2) xxxxxxxxxxxxxxx (“the parent” and “I”)

And governs the use and care of devices assigned to the parent’s child ( the “pupil”). This agreement covers the period from the date the device is issued through to the return date of the device to the school.

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

1. The school is lending the pupil a laptop (“the equipment”) for the purpose of doing school work from home
2. This agreement sets the conditions for taking a Aston Rowant Primary School laptop (“the equipment”)] home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

### 2. Damage/loss

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

I understand that I and the pupil are responsible for the equipment at all times whether on the school’s property or not.

If the equipment is damaged, lost or stolen, I will immediately inform the school and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don’t leave the device in a car or on show at home
- Don’t eat or drink around the device
- Don’t lend the device to siblings or friends
- Don’t leave the equipment unsupervised in unsecured areas

### 3. Unacceptable use

I am aware that the school monitors the pupil’s activity on this device.

I agree that my child will not carry out any activity that constitutes ‘unacceptable use’. This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language

I accept that the school will sanction the pupil, in line with our Behaviour policy, if the pupil engages in any of the above **at any time**.

**4. Personal use**

I agree that the pupil will only use this device for educational purposes and not for personal 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 my child locks the equipment if it's left inactive for a period of time
- 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 Mrs King on the email [office@aston-rowant.oxon.sch.uk](mailto:office@aston-rowant.oxon.sch.uk)

**6. Return date**

I will return the device in its original condition to the School Office within 5 days of being requested to do so. I will ensure the return of the equipment to the school if the pupil no longer attends the school.

**7. Consent**

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.


**Device loan agreement for staff**

**GRATITUDE    RESILIENCE    OUTREACH    WONDER    TRUST    HARMONY**  
*Growing together, rooted in God, enjoying fullness of life. (Colossians 2:1-7)*

## **1. This agreement is between:**

1) Aston Rowant Primary School (“the school”)

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 school.

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

1. The school is lending the employee a laptop (“the equipment”) for the purpose of working from home

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 agreement and my signature at the end of this agreement confirms that I have read and agree to these terms.

## **2. Damage/loss**

By signing this agreement 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 responsible for the equipment at all times whether on the school’s property or not.

If the equipment is damaged, lost or stolen, I will immediately inform Mrs King, and I acknowledge that I am responsible for full replacement costs. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

## **3. Unacceptable use**

I am aware that the school monitors my activity on the equipment.

I will not carry out any activity that constitutes ‘unacceptable use’.

This includes, but is not limited to:

Our acceptable use policy for ICT equipment,

- Accessing, creating, storing or linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Sharing confidential information about the school, its pupils, or other members of the school community
- Setting up any software, applications or web services on this device without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Carrying out any activity which defames or disparages the school, or risks bringing the school into disrepute  Using inappropriate or offensive language

I accept that if I engage in any activity that constitutes ‘unacceptable use’, I may face disciplinary action in line with the school’s policies on staff discipline/staff code of conduct

## **4. Personal use**

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

**GRATITUDE    RESILIENCE    OUTREACH    WONDER    TRUST    HARMONY**  
*Growing together, rooted in God, enjoying fullness of life. (Colossians 2:1-7)*

## 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 of time
- 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 school office via email: [office@aston-rowant.oxon.sch.uk](mailto:office@aston-rowant.oxon.sch.uk)

## 6. Return date

I will return the device in its original condition to the School Office within 5 of being requested to do so.

I will return the equipment to the school upon resignation, dismissal or if I leave the employment of the school for any other reason.

## 7. Consent

By signing this form, I confirm that I have read and agree to the rules and conditions above.


**GRATITUDE    RESILIENCE    OUTREACH    WONDER    TRUST    HARMONY**

*Growing together, rooted in God, enjoying fullness of life. (Colossians 2:1-7)*