LAWRENCE SHERIFF SCHOOL RUGBY

A Teaching School Hub

Online Safety Policy

Review date	Summer 2026	
Review period	Annual	
Next Review date	Summer 2027	
Reviewed by	Nicola Dandy	
Approving committee	Pastoral Committee	
Policy type	Non legislative	
Other related policies	Behaviour Policy Acceptable IT and Internet use Policy Anti-bullying Policy (Students)	Data Protection Policy Child Protection and Safeguarding Policy Code of Conduct (Staff) Complaints Policy

1. Aims 2
2. Legislation and guidance 2
3. Roles and responsibilities 3
3.1 The Trust Board 3
3.2 The Headteacher 3
3.3 The Designated Safeguarding Lead 3
3.4 The Director of IT 4
3.5 All staff and volunteers 4
3.6 Parents 5
3.7 Visitors and members of the community 5
4. Educating pupils about online safety 5
5. Educating parents about online safety 6
6. Cyber-bullying 7
6.1 Definition 7
6.2 Preventing and addressing cyber-bullying 7
6.3 Examining electronic devices 7
7. Acceptable use of the internet in school 9
8. Pupils using mobile devices in school 10
9. Staff using work devices outside school 10
10. How the school will respond to issues of misuse 10
11. Training 11
12. Monitoring arrangements 11
Appendix 1: Acceptable use agreement (pupils and parents/carers) 12
Appendix 2: LAWRENCE SHERIFF SCHOOL BYOD 6TH FORM STUDENT WIFI APPLICATION 14

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, visitors and trustees
- 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, 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.
- **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's) 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 pupils' 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 Trust Board

The Trust Board has overall responsibility for monitoring this policy and holding the Headteacher and senior leadership team to account for its implementation.

The Trust Board will co-ordinate regular meetings with appropriate staff to discuss online safety and to ensure the effective monitoring and logging of online safety logs by the designated safeguarding lead (DSL).

The Pastoral Committee hold the responsibility of overseeing online safety.

The Pastoral Committee will:

- Ensure that they have read and understand this Policy.
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (Appendix 2).
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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 and Senior Leadership Team 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 Lead (DSL) and Deputy Designated Safeguarding Leads (DDSL's) 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, 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 and Safeguarding Policy.

- Ensuring that any online safety incidents are logged via CPOMS and dealt with appropriately in line with this Policy.

- Ensuring that any incidents of cyber-bullying are logged via CPOMS and dealt with appropriately in line with the school Behaviour Policy.

- Updating and delivering staff training relating to online safety.

- Liaising with other agencies and/or external services if necessary.

- Providing regular reports on online safety in school to the Headteacher and Trust Board.

This list is not intended to be exhaustive.

3.4 The Director of IT

The Director of IT 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 pupils 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 IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

- A full security check and monitoring the school's IT systems is carried out on daily basis by Warwickshire Local Authority.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy.

  This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this Policy.
- Implementing this Policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (Appendix 2), and ensuring that pupils follow the school's terms on acceptable use (Appendices 1 and 2).
- Working with the DSL and DDSL's 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 / carers are expected to:

- Notify an appropriate member of staff, or the Headteacher, of any concerns or queries regarding this Policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendices 1 and 2).

Parents / carers 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
- The Lawrence Sheriff Online Safety site

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT 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.

4. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools.
- Relationships and sex education and health education in secondary schools.

Pupils in **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.

- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

By the **end of secondary school (Key Stage 5)**, 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, and throughout the wider school curriculum, such as PSHE, Citizenship, and Computing. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children and young people, victims of abuse and pupils 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.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use.

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

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

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour 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 school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying within their tutor groups as part of the school's wider PSHE programme.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, such as within their subject-specific areas, or as part the school's Anti–Bullying week, or Safer Internet day.

All staff, trustees 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 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 pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher can confiscate an electronic device if it is being misused, or if 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 Headteacher or appropriate member of the school's Senior Leadership team.
- 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 a school owned electronic device that they have confiscated where they believe there is a 'good reason' to do so.

Please note: No member of staff will directly search a pupil's electronic device If concerns were raised, the member of staff would refer to a DSL / DDSL who would then, if deemed necessary, seek advice from the police.
When deciding whether there is a 'good reason' to examine data or files on a school owned 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 Headteacher or DSL / DDSL 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 (or equivalent) 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 school's Behaviour Policy / Searching Students and Restraint by Staff 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 IT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

We recognise the growing role of Artificial Intelligence (AI) in education and everyday life. While AI can be a valuable tool for learning and creativity, it also presents potential risks.

Students must:

- Use AI responsibly and ethically when given permission to do so.
- Only use Copilot Chat
- Only have access to Copilot in Years 9-13
- Be aware of the risks of misinformation, bias, and privacy concerns when using AI-generated content.
- Not use AI tools to cheat, plagiarise, or complete assignments dishonestly.
- Never share personal or sensitive information with AI systems, as data security cannot be guaranteed.
- Seek guidance from teachers before using AI tools for schoolwork.

The school will:

- Educate students about the benefits and risks of AI.
- Monitor AI-related activities to ensure safe and age-appropriate use.
- Take disciplinary action if AI is used inappropriately or to compromise academic integrity.

8. Pupils using mobile devices in school

Pupils in Years 7 – 11 may bring mobile devices into school, but are not permitted to use them during the school day (8:45am-3:30pm) or during any after school clubs or educational visits unless given explicit instructions by a member of staff:

Sixth Form students are permitted to bring their own mobile electronic device and laptop into school, however this must be in line with the Acceptable Use Agreement (see Appendices 1 and 2).

Any breach of the Acceptable Use Agreement by a pupil may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring any memory sticks / external hard drives is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing 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 the Acceptable IT and Internet Use Policy.

Staff are permitted to occasionally use school IT facilities and devices for personal use, subject to certain conditions set out in 5.2 of the Acceptable IT and Internet Use Policy.

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

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use of IT (Students). 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 IT 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 / Acceptable use of IT (Staff). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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 and young people 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 DDSL 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.

Trustees 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

The DSL logs behaviour and safeguarding issues related to online safety via CPOMS.

This Policy will be reviewed annually by the Deputy Headteacher (Pastoral). At every review, the Policy will be shared with the Pastoral Committee. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix 1: Acceptable use agreement (pupils and parents/carers)

Acceptable Use of IT Agreement (Students)

As part of the school's IT programme, we offer pupils access to school computers and to the Internet. Before being allowed to use these resources, all pupils must obtain parental permission and both they and you are requested to sign the Confidential Personal Information Sheet as evidence of your approval and their acceptance of the school rules on this matter.

Access to the Internet enables pupils to explore thousands of libraries, databases and forums while exchanging messages with other Internet users throughout the world. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. Lawrence Sheriff School does not condone the use of such materials and will use its best endeavours to prevent access to all such inappropriate materials.

Whilst our aim for computer use and Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and carers of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

During school, teachers will endeavour to guide pupils towards appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

We should be grateful if you would read the following guidance notes and then complete relevant section on the personal information form and return it with your acceptance papers - **if permission is not given, pupils will be barred from using the computer network and the Internet**. If you do not wish your son/daughter to have access to the Internet, please would you confirm this in writing.

Pupils will be provided with a personal Gmail account which will be used by them to communicate with teachers and fellow pupils. This account should not be used by parents to communicate with the school.

SCHOOL RULES ON THE USE OF COMPUTERS AND THE INTERNET

- Pupils are responsible for good behaviour on the school computers and the Internet just as they are in a classroom or a school corridor. General school rules apply.
- The Internet is provided for pupils to research classroom projects and communicate with others (E-mail). Parents' permission is required. Remember that access is a privilege, not a right and that access requires responsibility.
- Individual users of computers and the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards and will honour the agreements they have signed.
- Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.
- Pupils are expected to make best endeavours to ensure malicious code is not introduced onto the computers in the school.
- Pupils should logon using only their own school logon information (do not use logon information belonging to someone else) and should not divulge personal logon details to others.

- Pupils should not use computers in any way that is deemed by the school now or in the future, to be detrimental to others or to the smooth running of the school's computer infrastructure.

The following are not permitted:

1. Sending or displaying offensive messages or pictures.
2. Using obscene language.
3. Harassing, insulting or attacking others.
4. Damaging computers, computer systems or computer networks.
5. Violating copyright laws or copying/pasting others' work without noting the source.
6. Bringing into school, in electronic form, any materials that would be unacceptable on paper.
7. Intentionally wasting limited resources.
8. Using the Internet for any illegal purpose.

Sanctions:

1. Violations of the above rules will result in a temporary or permanent ban on network and Internet use.
2. Additional sanctions may be added in line with existing practice for inappropriate language or behaviour.

Please see below for the agreement details for the use of email and the internet.

By completing and signing the personal information sheet you are agreeing to the following:

Pupil

As a school user of the Internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Parent

As the parent or legal guardian of the pupil, I grant permission for my son/daughter to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring information and media.

If you do not wish your son/daughter to have access to the computer network and the Internet, please confirm this in writing and attach it to your son's/daughter's personal information sheet. Thank you.

Appendix 2: LAWRENCE SHERIFF SCHOOL BYOD 6TH FORM STUDENT WIFI APPLICATION

Guidelines:

- Students participating in B.Y.O.D. must adhere to the Acceptable Use of IT Agreement (Students).
- Students are responsible for their own device; the school accepts no liability for damage, loss or theft.
- Students are responsible for ensuring their device is suitably charged. Due to health & safety reasons, students do not have permission to charge their device at school.
- A device must only be used for educational purposes as outlined in the Acceptable Use of IT Agreement (Students).
- Each teacher has the discretion to allow and regulate the use of devices in the classroom and on specific projects. Members of staff reserve the right to confiscate a device which is being used inappropriately.
- The device must be running original and legal copies of the operating system and any other software or app. If they are not original and legal copies, then they should not be connected to the school network. Approved devices must be in silent mode while on school grounds, unless otherwise allowed by a teacher. Headphones may be used with teacher permission.
- Devices may not be used to contravene exam conditions be they internal or external assessment.
- Devices must not be used to record, capture images, video or audio of other students or staff without their consent. Images, video or audio must not be shared or posted on a social media site without the consent of those involved.
- Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.
- Fair use of the school network is permitted during school hours, however the following are not permitted and not limited to: downloading of illegal or copyrighted material, use of streaming websites, any method to obfuscate internet usage, and use of a device and the school network to abuse others or circulate unsuitable material is also unacceptable.

DECLARATION

I confirm that I have read and understood the Acceptable Use IT Agreement and will adhere to the guidelines set out above. I hereby declare that I shall use the WiFi access allocated to me as per the existing policies of Lawrence Sheriff School IT facilities. I shall not reveal my WiFi Credentials to anyone, will not use Proxies or VPN's to mask my internet usage, and I am solely responsible for the activities done through my internet access. I acknowledge that this WiFi is the property of the local authority who reserve the right, as part of their Safeguarding and Prevent obligations, to monitor all traffic from this device when using their WiFi connection. Any misuse may result in permanent disqualification from using this service.

Signature: _____ Date: _____

PRINT NAME:_____

EMAIL:_____

Configuration details of the Device on which WiFi access is requested:
(only one device per student will be granted WiFi access)

Device Type: Windows Laptop / Mac Book / iPad / Android Tablet / Chrome Book

Device Make (Apple, Samsung, etc):_____

Device Model and OS:_____

MAC Address (Private Address Not Allowed):_____
(Unauthorised MAC addresses will be blocked permanently)