**Leigh St. John's C.E. Primary School**
Kirkhall Lane
Leigh
WN7 1RY
Headteacher: Mrs E. Lightfoot

# E-Safety
# POLICY

| | |
|---|---|
| **Developed in consultation/advisory role with:** | Governing Body, SLT, Staff, Pupils, Parents, LA, external services |
| **For use by:** | Pupils, Staff, Parents, Governors, and external service providers/users. |
| **Reviewed:** | Full Governing Body – |
| **Agreed by:** | All staff |
| **Next policy review date:** | Spring Term 2026 |
| **Signed Chair of Governors:** | Mrs K Partington |
| **Date:** | February 2023 |

## 1. Introduction

This policy is to be used in conjunction with the school's Safeguarding and Child Protection Policy, Prevent Statement, Behaviour and Relationships Policy and Computing Policy.

St. John's E-Safety Policy is compliant with the approved Wigan Safeguarding Children Board (WSCB) and Guidance for working with adults and children / young people who are vulnerable to the messages of violent extremism.
It promotes effective practice in order to protect pupils and educate them in responsible computing and internet use. The E-Safety Policy is part of the Strategic School Impact Plan and relates to other policies, including those for Computing, Behaviour and for Safeguarding and Child Protection.

## 2. Rationale

The purpose of this policy is to:

• Set out the key principles expected of all members of the school community at Leigh St. John's CE Primary School with respect to the use of COMPUTING based technologies.

• Safeguard and protect the children and staff of Leigh St. John's CE Primary School and comply with GDPR (General Data Protection Regulation).

• Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.

• Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

• Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.

• Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

• Minimise the risk of misplaced or malicious allegations made against adults who work with students.

## 3. Use of the internet

The Internet is widely recognised as an essential resource to support teaching and learning. The national curriculum requires pupils to use technology purposefully, safely and responsibly to create, organise, store, manipulate and retrieve digital content. At KS2, specifically, pupils are required to be taught about computer networks, including the internet, exploring the opportunities they offer for communication and collaboration. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning, such as touch screen tablet devices. Computer skills are vital to access life-long learning and future employment; indeed, computing is now seen as an essential life-skill.

Children and young people have access to the Internet from many places, home, school, friends' homes, libraries and most predominantly through mobile devices such as smart phones, tablets and game consoles. Schools have a number of services to help ensure that curriculum use is safe and appropriate; however, access out of school does not usually have these services and has a range of risks associated with its use.

Some of the specific harms which children can experience online include:

**Content**:

- Exposure to illegal, age-inappropriate & harmful images/video or other content
- Exposure to radicalising content
- Exposure to harmful content, such as suicide content

**Contact**:

- The risk of being subject to grooming and subsequently abuse
- knowledge
- Cyber-bullying
- Youth-produced sexual imagery (sexting)
- Identity theft and sharing passwords

**Conduct**:

- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- The sharing/distribution of personal images without an individual's consent or unauthorised access to/loss of/sharing of personal information

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety policy is used in conjunction with other school policies (e.g. behaviour and relationships, anti-bullying and safeguarding & child protection policies). As with all other risks, it is impossible to eliminate these completely. It is therefore essential, through good computing teaching and provision, to build pupils' awareness to and resilience to the specific dangers which they may be exposed, so that they have the confidence and skills to face and deal with these.

Schools are ideally placed to help children and young people learn to become e safe. This policy is designed to ensure safe internet use by pupils in school, but also while on-line at home and elsewhere etc.

## 4. Use of internet filtering, monitoring arrangements and incident management in school

Schools in England (and Wales) are required *to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate* *levels of filtering*. The Department for Education published the revised statutory guidance 'Keeping Children Safe in Education' in September 2022 for schools and colleges in England which includes some important additions about online safety. It specifies that *governors/trustees should ensure that the school/college leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified*. Children should not be able to access harmful or inappropriate material from the school IT system. However, schools need 'to be careful that over blocking does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding'.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. At St. John's C.E. Primary School we work in partnership with Wigan Council, Wigan Safeguarding Children's Board (WSCB)/Wigan Safeguarding Partnership and Benchmark North, our ICT Technical Support Team, to ensure systems to protect pupils are frequently reviewed and improved.
We will take all reasonable precautions to ensure that users access only age appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school endeavours to ensure that pupils use the Internet in a safe and controlled way. The school cannot accept liability for the material accessed, or any consequences of internet access.

Our filtering system, provided through Benchmark North is 'Cyren' which is based within school. That is further protected through Benchmark North's preferred cloud-based DNS filter. Our monitoring system is 'Senso Cloud Classroom Management System'.

Our primary web-filtering is applied at network level and therefore doesn't rely on any software or client agents. It includes age appropriate, differentiated filtering, including the ability to vary filtering strength appropriate to the age and role of the user e.g., YouTube can be enabled for staff but not for pupil use. The school can manage its own approved and block lists. Our system isn't limited to filtering just HTTP traffic and includes the blocking access to inappropriate content via mobile and app technologies (on the school's network).

- In the event of the Technical Staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to Benchmark North on 01942 492479.
- Requests from staff for sites to be added or removed from the filtered list will be considered at the appropriate senior level. If the request is agreed, this action will be recorded, discussed by the E-Safety Leader and presented to governors with reasons for the removal. The use of the filtered sites will then be monitored in conjunction with the ICT Misuse Protocol (appendix 3).

Senso Cloud Classroom Management System is installed on all school computers and iPads including those loaned to staff and is updated regularly. This digital system works by making daily captures of violations and sorts these into specific categories. The headteacher has access to all logged violations and escalates these accordingly through the agreed channels.

Monitoring is done by analysing keyword uses against these categories: adult content, bullying, child sexual exploitation, discrimination, drugs/substance abuse, extremism, IWF Keywords (IWF = Internet Watch Foundation), IWF URLS, self-harm, sexting, suicide and violence.

School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy / e-safety Agreement.

## 5. Security

- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- Data breaches are reported to our Data Protection Lead (DPL) Mrs Pauline Jones. Our Data Protection Officer (DPO) is Jo Buckley and if a matter needs escalating it would then be referred to the Information Commissioners Office (ICO).
- Any safeguarding incidents are reported to the Designated Safeguarding Lead (DSL) Mrs Lightfoot or to Mrs Hughes, Mrs Hatton or Mrs Boneham (Deputy Safeguarding Leads)
- All the e-safety incidents are reported to the Headteacher and Computing Leader.
- All laptops and PCs on the school's network require the user to agree to the school's acceptable use on start-up.
- Pupils will only publish work within an appropriately secure environment: seesaw, blog, g-suite, office365 and school approved cloud storage systems.
- Staff are required to preview websites before use [where not previously viewed or cached].
- All staff users know and understand what the 'rules of appropriate use' are, GDPR compliance and what sanctions result from misuse – through staff meetings and teaching programme.
- Regular advice and information on the procedures for reporting offensive materials, abuse/ bullying etc is made available to pupils, staff and parents.
- The school network requires unique, individual log-in credentials and these are audited for all users.
- Storage of all data within the school will conform to the GDPR requirements.
- Staff will use Microsoft OneDrive (part of Microsoft 365 apps for faculty) to save and hold any relevant data about pupils. Usb storage devices / pen drives are not permitted.
- Staff access to the schools' management information system (SIMS) is controlled through a separate password for data security purposes;
- It is regularly made clear to staff and pupils that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network. Learners are always encouraged to log off when they have finished working on a device and know the expected behaviour if they acquire a device that is still logged into another child's account – log off and log on with their own credentials.
- On the school's network is a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas when not publishing to seesaw or other approved cloud storage systems.
- staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- The school does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children.
- The school has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- The school ensures that it has a data protection agreement in place with all of its third-party software providers e.g. Tapestry,

## 6. Awareness and Training

In demonstrating our commitment to protecting our pupils online, our school is a subscriber to the National Online Safety Certified School Programme, which provides access to all staff, governors and parents to online safety training courses, webinars, guides, lesson plans and updates to keep children safe online.

Parents and carers' attention will be drawn to matters regarding e-safety policy in weekly newsletters and on the school website.

- Parents and carers will be encouraged to refer to the practical e-safety guides provided on the school website.
- A partnership approach with parents and carers will be encouraged. This includes demonstrations, practical workshop sessions and suggestions for safe Internet use at home.

For further advice, parents and carers can visit:

- The parent portal of National Online Safety Certified School
- www.thinkuknow.co.uk
- https://www.saferinternet.org.uk
- www.kidsmart.org.uk
- www.bbc.co.uk/cbbc/topics/stay-safe
- www.thinkuknow.co.uk/5_7/hectorsworld

For Guidance on activating Parental Controls, parents and carers can visit:

- www.thinkuknow.co.uk/parents/Primary/Tools/Parental-controls

## 7. Roles and responsibilities

The following information outlines the Online Safety roles and responsibilities of individuals and groups within the school:

**Governors**:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Full Governing Body receiving regular information about E-Safety incidents and monitoring reports. The designated governor with the responsibility for safeguarding also oversees matters regarding E-Safety. This role includes:

- regular meetings with the Designated Safeguarding Leader and E-Safety Leader
- attend, where possible any parent or staff E-Safety training
- regular monitoring of E-Safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors meetings

**Headteacher and Senior Leaders**:

In accordance with the updated Keeping Children Safe in Education (KCSIE) 2022, the Designated Safeguarding Lead (DSL), who is also the headteacher, maintains the overall responsibility for online safety.

- The DSL undertakes regular e-safety training through the National Online Safety portal and disseminates information across the staff team.
- The Headteacher/Senior Leaders are responsible for ensuring that the E-Safety Leader and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Leader. The Headteacher and another member of the Senior Leadership Team should be aware of the

procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff (Appendix 3 - ICT Misuse / E-Safety breach Reporting Protocol).

**E-Safety Leader**:

- takes a leading role in establishing and reviewing the school e-safety policies/documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- provides training and advice for staff;
- ensures that regular checks are made to monitor that the filtering methods in place are appropriate, effective and reasonable;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments (E-Safety Incident Report Log Appendix 3);
- reports regularly to the DSL and Senior Leadership Team;
- attends relevant Governor meetings.

The E-safety Leader is also the administrator of Senso (the school's monitoring system) and will conduct routine checks of website logs to check for any violations. If any serious violation is discovered, they refer to the school's **Flowchart for responding to an E-Safety Concern** contained in Appendix 2.

**Technical Staff:**

The ICT Technician and Computing Leader are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policies and guidance and as advised by Becta;
- that users may only access the school's networks through a properly enforced password protection policy;
- jointly led e-safety work in school alongside the E-Safety Leader, including organising Internet Safety Days;
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- that the use of the school network is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Leader for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

**Teaching and Support Staff**

Teachers and other staff members are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read, understood and signed the school Responsible Internet User Agreement – Appendix 1);
- they report any suspected misuse or problem to the E-Safety Leader /Headteacher/ Computing Leader for investigation/action/sanction;
- digital communications with pupils (seesaw/email/blog/Tapestry/Twitter) should be on a professional level and only carried out using official school systems (Responsible Internet User Agreement – Appendix 1);

- e-safety issues are embedded in all aspects of the curriculum and other school activities (Long Term Planning);
- children/pupils understand and follow the school e-safety Responsible Internet User Agreement – Appendix 1);
- children/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor computing activity in lessons and extra-curricular school activities;
- they are aware of e-safety issues related to the use of mobile phones, cameras and mobile devices and that they monitor their use and implement current school policies with regard to these devices;
- in lessons where internet use is pre-planned children/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- any Apps have been appropriately screened and approved for use in lessons;
- they are responsible for maintaining an appropriate digital footprint – they will act responsibly when using social media platforms.

### Designated Safeguarding Lead/Child Protection Officer

The DSL and deputy DSL will be trained in e-safety matters and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate content;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber-bullying.
- Youth-produced sexual imagery (sexting)
- Online child-on-child abuse, including sexual violence and sexual harassment.

The DSL has an essential role to play in both preventing online child-on-child abuse and responding to any concerns when they occur, even if they take place offsite and ensures that there are appropriate systems in place to support and evidence this.

The DSL is responsible for ensuring the school's child protection policy and wider safeguarding policies specifically address online safety, especially with regards to online child-on-child abuse, relationships on social media and the use of mobile and smart technology.

### Children / Pupils

- are responsible for using the school ICT systems and mobile technologies in accordance with the Responsible Internet User Agreement (Appendix 1);
- are responsible for reporting abuse, misuse or access to inappropriate materials and know how to do so.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school if related to their membership of the school.

**Community Users**

Community Users who access school ICT systems and devices will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

**Parents/Carers**

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, weekly newsletters, letters, website, Tapestry and providing free access to the National Online Safety Portal. Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to parents' sections of the website and Tapestry and on-line student records;

## 8. <u>Safe and appropriate use of mobile technologies</u>

- Mobile technologies such as iPads, iPods and laptops are fully integrated into the wide expanse of learning opportunities provided to facilitate learning across the whole curriculum.
- Appropriate use of these devices will be promoted to staff through an on-going programme of training and taught to pupils as part of their learning of e-safety.
- iPads and associated 'Apps' (Application Computer Programs for mobile devices) will be carefully examined and scrutinised for educational benefit and a risk assessment will be carried out before use in school is allowed.
- iPads will be managed centrally by the computing lead through the Mosyle Mobile Device Management System meaning that pupils will not be able to install content themselves. Restrictions will also be enabled on all pupil devices.
- Mobile phones will not be used by staff during lessons or during directed teaching time unless appropriate arrangements have been made; for example, a role play phone call or to play music via a Bluetooth enabled speaker.
- Pupil mobile phones are restricted to Y6 pupils whose parents have given consent for them to walk home from school alone. These devices must be placed on silent when handed in and are kept locked in the Y6 class safes until the end of the school day.
- All visitors entering school are requested to keep their phones on silent.

The following uses of mobile technologies, whether or not owned by the school are not permitted:

- Harming or embarrassing another person through the use of text, sound and/photos;
- Bullying or intimidating another person through text, sound and/photos.

## 9. <u>Use of digital imagery and video</u>

I Pads and associated apps have created significant benefits to learning, allowing staff and pupils instant use of images e.g. for the collection and sharing of ongoing assessment information, the creation of e-books, the uploading of pupil work to a class / pupil online journal etc.

- When using digital images, staff should inform and educate children/pupils about the risks associated with the taking, use of, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites, including blogs.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not

be used for such purposes. However, should circumstances require, images may be taken on staff owned equipment provided that at the first available opportunity they are transferred to the school's network / storage device and deleted from the staff device.

- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, twitter, blog or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written consent from parents or carers will be obtained before photographs of pupils are published on the school website/twitter account/blog. Photographs will not be named and in other places, no full names will be used on the website.

## 10. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

**The school must ensure that:**

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Responsible persons are appointed/identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs).
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

**Staff must ensure that they:**

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When  personal data is stored on any portable computer system, memory stick or any other removable media:

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

## 11. **Computing Curriculum**:

Our computing curriculum aims to teach pupils the skills associated with three distinctive strands:

- Information Technology
- Computer Science
- Digital Literacy.

The digital literacy knowledge, skills and understanding permeate through the entire curriculum. They also feature in discreet computing lessons and support pupils to learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour and develop effective strategies for staying safe and making a positive contribution online.

Our computing curriculum equips the children with the skills and understanding they need to be able to safely navigate our connected online world.

The curriculum covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page / blog may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post photos or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- [for older pupils]to understand why and how some people will 'groom' young people for sexual reasons;

- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

## 12. Email guidelines for staff and pupils

- Pupils, staff and Governors may only use approved e-mail accounts on the school system.
- Pupils must be made aware of how they can report offensive emails and whom they should report violations to. The named person would be the headteacher.
- Pupils must immediately tell a teacher if they receive offensive or inappropriate e-mail.
- In e-mail communication, pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.

## 13. Tapestry Online Learning Journals

Tapestry Online Learning Journal is the school's primary method for communicating to parents & carers ongoing information regarding children's learning and development. Written requests from parents & carers and signed user agreements are obtained before users are provisioned to access the online site / App. This section is designed to ensure that all 'users' of Tapestry, including Parents and Carers, display appropriate behaviour when commenting on teacher posts or when posting a comment themselves.

1. I will be polite, and I will never post anything that could hurt anyone.
2. I will always show respect when writing comments.
3. I will always remember that posts must reflect a celebration of my child's learning and development.
4. I will acknowledge posts by 'liking' or commenting.

## 14. Class Blogs – leighstjohns.net

At Leigh St. John's, blogging involves pupils working on a blog whilst in school and also at home. To be able to post, pupils are required to log into the blog either using an individual sign in or a class sign in (EY and KS1). The individual sign in is utilised with Year 3 pupils onwards and this gives more ownership to each pupil. Our blog platform allows accounts to have different permissions. Contributor is the lowest level that allows a user to post. A contributor can submit a post for review; however, this will need to be authorised by the admin before it appears on the blog. Any other permission level above that of 'Contributor' is assigned to staff members and allows posts to be viewable as soon as the individual clicks 'Submit'.

Using a blog safely is the most important thing about being a blogger. At Leigh St. John's, the following rules apply to minimise any risks and ensure that pupils stay safe whilst blogging.

Don'ts:

1. Never give away any personal information about your location or identity.
2. Post your full name - first names are OK though.
3. Don't post pictures of yourself without specific permission from your teacher or parents.
4. Never give out your log in details to anyone.
5. Don't use text language in your posts

Do's:

1. Post about whatever you like.
2. If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.
3. Comment on other people's posts too. Blogging is about commenting and posting! It is advised that everyone leaving comments, including children and staff, should follow the 'quality comments' criteria:

    - Say something positive
    - Ask a question
    - Suggest an improvement

4. If your post doesn't appear straight away, you teacher might be busy, do be patient.
5. Try to post about things that your audience would like to read.
6. If you see anything that shouldn't be on your screen, do tell your teacher or parents immediately.
7. Do visit other class blogs regularly to read and comment. This helps people come back to your blog.
8. Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.
9. Always tag your posts with your first name and include key words specific to your post.

### 15. School Twitter - @LeighSTJOHNSsch

Twitter will not be used to engage with individual parents directly; however, important announcements / notices and celebrations of pupils' work will be posted on the school's main and class twitter feeds. Staff personal accounts will belong to the individual staff member and they will be solely responsible for their tweets and unless staff are linking their personal account to class blogs, direct reference to the school should be avoided.

Any Tweets from the official school account will be grammatically correct and will not contain text language like lol, gr8 or l8r. Some tweets may contain hashtags. Hashtags are things you can add to the end of your tweets like #edchat #PrimaryRocks that enable tweets to be added to a collection of other related tweets that are generally viewed by more people.

In order to safeguard the pupils at Leigh St. John's C.E. Primary School, no names of pupils will be used alongside any pictures of pupils. Leigh St. John's seeks photographic consent of all the pupils. Tweets sent by the school will adhere to this list. If tweets are sent inviting people to view a blog post by an individual pupil, only their first name will be used.

Anyone can follow the school's Twitter account. Weekly checks will take place by a member of the SLT to check recent followers. Any user following the school account that is deemed unsuitable or not adding any value to the school will be blocked. A member of the SLT will make this decision on a case-by-case basis. Parents will be encouraged to follow the official school account and relevant class twitter accounts to receive the information the school is posting up to Twitter.

### 16. School Website

- The Headteacher and Deputy Headteacher take the overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained; however, other staff members have contributor access so that they are able to publish the information which falls under their roles and responsibilities.
- The school web site complies with the statutory DfE guidelines for publications;

- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use the main office email address as contact, enquiries@admin.leighstjohnsprimary.wigan.sch.uk
- Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geo-data in respect of stored images.

## 17. Asset Disposal

When school electronic devices reach the end of their lifespan, we ensure that suitably certified suppliers, approved by our IT Technical Support Team are procured to dispose equipment. On completion, we are issued a certificate of destruction.

## 18. Incident Response

How will school respond?

Incidents should be reported to the school's DSL, e-safety leader, or equivalent member of staff, who can assess the severity of the report in order to determine what course of action needs to be taken.

If it is considered that the pupil involved faces an immediate risk due to the incident, school will:

- Collect all of the relevant and available evidence.
- Inform child protection services, LADO and Wigan Safeguarding Children Board
- Allow any external agencies, e.g. child protection services or the police, to complete their investigation and take any necessary steps once it has concluded.

If the incident is illegal but does not pose an immediate risk to the child involved, schools should collect all of the available evidence and either encourage the pupil to report the incident using the CEOP form or help the pupil to use the CEOP form. If the incident is more general in nature, then the school might consider reporting the incident to the Internet Watch Foundation (IWF) on behalf of the pupil, as the form that would need to be completed is not child-friendly. If a report is made, school should await a response and act accordingly once this has been received.

If a reported e-safety incident is not illegal, e.g. cyber bullying, procedures should still be followed to ensure that the pupil is assured that their report is being taken seriously. Depending on the nature and severity of the incident, it might be appropriate to take some of the following actions:

- Block reported webpages
- Notify the parents of the pupil who has reported an incident or, in cases where a pupil is making a report against another pupil, inform the parents of the alleged perpetrator
- Provide any necessary sanction

No matter the severity of the incident that has been reported, school staff should continue to monitor the situation even after it has reached a conclusion – this is especially important in cases of cyber bullying where inappropriate behaviour may continue.

- Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children will be reported to the LADO within one working day in accordance with Wigan Safeguarding Board advice.
- Any complaint about staff misuse must be referred to the DSL / headteacher and if the misuse is by the headteacher it must be referred to the Chair of Governors in line with Wigan Safeguarding Board Child Protection procedures.
- Pupils, parents & carers and staff will be informed of the complaint's procedure.

- Breaches of Acceptable Use of the Internet will be dealt with swiftly and effectively. The school takes guidance from the '**Wigan Safeguarding Children Board**'
- In the event of a potential e-Safety concern or incident the school will follow the steps outlined in the **Flowchart for an E-Safety Concern** contained in Appendix 2.

Following an e-safety incident

Following an e-safety incident, it is important to record all of the procedures that were followed to ensure they comply with the school's E-safety Policy, and to see if any additional and effective steps were taken to deal with the incident that could be added to the E-safety Policy during the next policy review. Information about e-safety incidents and how they were reported and dealt with will also be useful in supporting staff training

All incidents will be recorded in the school's e-safety log (file).

This Policy should be used in conjunction with the following:

Child Protection Policy
Relationships and Behaviour Policy
Data Protection Policy

# Appendix 1

## Part a) Responsible Internet User Agreement:

### Staff, Pupils & Parents/Carers, Governors, Visitors and Students

**These rules help us to be fair to others and keep *everyone* safe.**

- I will use only my own network login and password (or in the case of a pupil, **my class** network login and password), which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission as these could threaten the integrity of the school ICT systems.
- I will only e-mail and open attachments from people I know, or in the case of a child, that my teacher has given permission for.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or to arrange to meet someone.
- If I see anything I am unhappy with or someone sends me a message I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails, blogs and the Internet sites I visit.
- I will not use social networking sites (Facebook etc.) on any school devices.
- I will not use the Internet for personal gain, gambling, political purposes, or advertising.
- I will only use the Internet for my learning, or in the case of staff, governors, visitors and students on placement, for my professional activities.
- When using mobile devices on site including mobile phones, iPad's, iPod's, tablet PC's and notebooks, **ONLY** devices **owned by the school** can access the secure wireless network. The network key and password should remain private and exclusive to school staff. Other adults wishing to use their personal devices on site must use their built in enabled 4G connections.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet, computers or other mobile device.

  The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited and e-mails sent or received.

  The school strongly recommends that children do not use social network sites such as Facebook, WhatsApp, Instagram, TikTok, Facebook messenger, Houseparty, Twitter, Yolo and Snapchat, as these sites carry age-restriction and pose a risk to children. Social network sites have no place at our school for the discussion of **school issues** and therefore school staff should not be approached online or invited to become 'friends.'

The following table shows a summary of the key permitted and unpermitted information and communication technology activities:

|  | Staff & other adults |  |  |  | Pupils |  |  |  |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Allowed. | Allowed at designated times. | Allowed with Head teacher permission. | Not allowed. | Allowed. | Allowed when directed during lessons. | Allowed with teacher permission. | Not allowed |
| Mobile phones may be brought to school. | * |  | * |  |  |  |  | *<br>except for Y6 pupils where consent has been obtained and they walk home independently. |
| Use of mobile phones in lessons. |  |  | * |  |  |  |  | * |
| Use of mobile phones in social times. |  | * |  |  |  |  |  | * |
| Use of mobile phones to take photographs. |  |  |  | * |  |  |  | * |
| Use of school iPads, iPods to take photos or video. | * |  |  |  |  | * |  |  |
| Use of school G-Suite & Office365 App to collaborate, blog, instant message, find information and save work. | * |  |  |  |  | * |  |  |
| Use of school mobile devices and computers to browse the internet. | * |  |  |  |  | * | * |  |
| Use of school mobile devices and computers to access and work on APPS and other programs. | * |  |  |  |  | * | * |  |
| Use of school email for personal emails. |  |  | * |  |  |  |  | * |
| Use of IMessage and Face Time. | * |  |  |  |  |  |  | * |
| Use of QR code decoding software to access a url. | * |  |  |  |  | * | * |  |
| Use of **secure** personal file storage / sharing applications e.g. seesaw, onedrive, google drive | * |  |  |  |  | * | * |  |

# Appendix 1

## Part b) Responsible Internet User Agreement (STAFF AND GOVERNORS ONLY)

**These rules help us to be fair to others and keep everyone safe outside of school hours.**

Outside of school working hours we as professionals have instant access to many powerful mobile devices that open up new opportunities for effective communication and collaboration e.g. social networking sites, video calling, file sharing, online collaboration and much more. In our roles as teachers and governors we have a duty of care to protect children as well as a wider responsibility to protect the integrity of the school and its ethos. We must ensure that we behave responsibly and professionally when using such technologies to communicate with others when out of school. The following code of conduct has been designed to guide us in safe Internet use when we are not in school:

- When logged into social networking sites such as Facebook, Instagram, Snapchat, Twitter etc. **DO NOT** interact with any current or past (under 16 years of age) pupils.
- When logged into social networking sites such as Facebook, Instagram, Messenger, Snapchat, Twitter, Pinterest etc. **DO NOT** upload pictures that have been taken during the school day or on school events of colleagues or pupils. (Always seek permission from colleagues when uploading photos taken of them during social events outside of school hours). Kindly ensure that any photos that you post of yourself or your colleagues **cannot** bring the school name into disrepute!
- It is strongly advised that you do not accept parents or carers as 'friends' on social networking sites. If you are already pre-existing 'friends' ('liked by') with any parents or carers **DO NOT** discuss school related issues.
- When using school mobile devices that have been loaned to you e.g. iPad and laptop, ensure that emails and text messages are constructed with the same professional tone as those which leave the school office on corporate school letter headed paper. **ALWAYS REFRAIN** from using text abbreviations in email correspondence and **NEVER** attach sensitive pupil data as attachments. Egress secure email should always be used for exporting sensitive and confidential data.
- Only school approved cloud storage should be used to store data: OneDrive and google drive.

Unsuitable/inappropriate activities

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

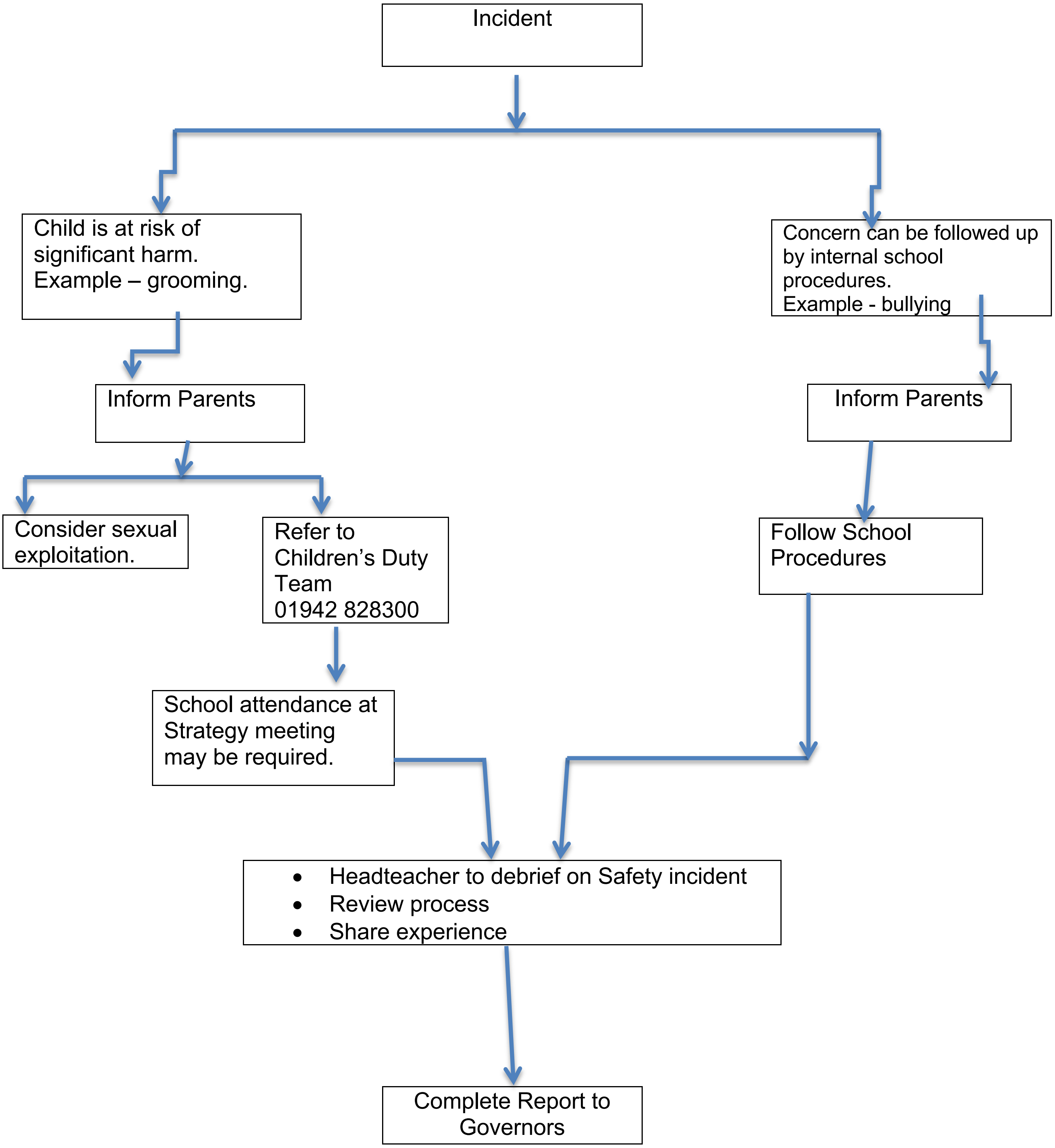
| | Acceptable. | Acceptable at designated times. | Acceptable for nominated users. | Unacceptable. | Unacceptable and illegal. |
|---|---|---|---|---|---|
| Use of video calls e.g. TEAMS, Zoom | * | | | | |
| Use of social networking sites | | * | | | |
| File sharing | | * | | | |
| Online shopping/commerce | | * | | | |
| Online gambling | | | | * | |
| Online gaming (non educational) | | | | * | |

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

# Appendix 2

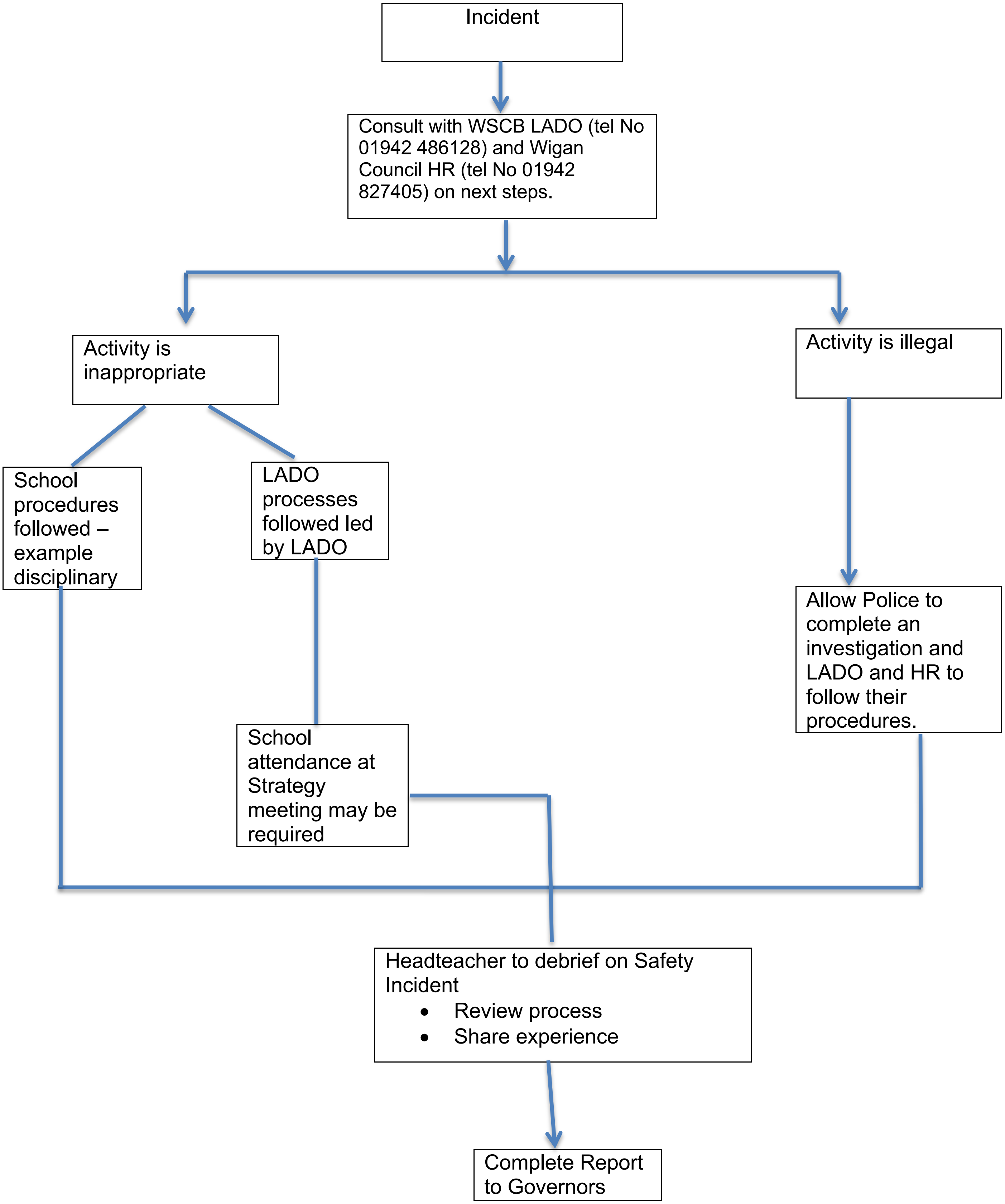
## **Flowchart for an E-safety Concern**

Procedure (CHILD) – Schools and Settings e-safety Policy incidents.


Incident
Child is at risk of significant harm. Example – grooming.
Concern can be followed up by internal school procedures. Example - bullying
Inform Parents
Inform Parents
Consider sexual exploitation.
Refer to Children's Duty Team 01942 828300
Follow School Procedures
School attendance at Strategy meeting may be required.
• Headteacher to debrief on Safety incident
• Review process
• Share experience
Complete Report to Governors

## **Flowchart for an E-safety Concern**

Procedure (STAFF) – Schools and Settings e safety Policy incidents.



Incident

Consult with WSCB LADO (tel No 01942 486128) and Wigan Council HR (tel No 01942 827405) on next steps.

Activity is inappropriate

Activity is illegal

School procedures followed – example disciplinary

LADO processes followed led by LADO

School attendance at Strategy meeting may be required

Allow Police to complete an investigation and LADO and HR to follow their procedures.

Headteacher to debrief on Safety Incident

- Review process
- Share experience

Complete Report to Governors

# Appendix 3

**Agreement for the long-term loan of an electronic mobile device, including Laptop and i Pad/**

## (STAFF ONLY)

## General

- The laptop or iPad detailed on this form is agreed as a long-term loan to the named member of staff whilst in the service of this school. As part of this agreement the member of staff undertakes to make best endeavours to keep the equipment in good condition and safe. The above equipment must be returned to the school when the member of staff leaves the school's employment.
- The laptop or iPad is loaned for the sole, exclusive use of the members of staff (who have accounts) for professional purposes.
- The laptop or iPad MUST be kept secure at all times.
- The Computing Leader or Internal Audit may also request your mobile device at any time in order to monitor usage.
- Except with prior explicit written permission from the Headteacher and Computing Leader, resources must not be used for school related commercial purposes, or monetary gain.
- Your device should be password protected. You are prohibited from disclosing your password to any individuals. You must safeguard your user area and its contents and will be responsible for any misuse. You may not search for, access, copy, or use passwords belonging to other people.
- It is your responsibility to ensure that all data on the device is regularly and securely backed up to a school approved cloud storage system.
- USB portable devices should not be used under any circumstances.
- Additional hardware, software, music and APPS may only be installed onto the device with permission from the Headteacher and Computing Leader.
- The laptop or iPad is loaned to the member of staff for professional purposes and therefore additional hardware, software, music, device drivers and APPS should only be installed by the school's Computing Leader and Headteacher in accordance with the appropriate licences issued within Apple School Manager.
- Internet usage is subject to the school E-safety Policy and to the ***Responsible Internet User Agreements*** previously signed.
- You should check with your Computing Leader and Benchmark North Technician that appropriate anti-virus software has been installed on your portable device and that it is regularly updated.
- You may not copy any software from the device to any other machine outside of school's control (without written permission from a member of the SLT).
- Pre-installed software must not be removed or the device reconfigured in any way (without written permission from a member of the SLT).

## Insurance

- The mobile device (laptop / iPad) and the associated equipment listed are on the school's asset register and are covered under the school's insurance. This insurance covers the use of the device at the teacher's home. The insurance does not cover damage/loss in transit between the school and the teacher's home. The device must not be left unattended in a vehicle at any time.

## Repair and Maintenance

- The device (laptop / iPad) and the associated equipment listed will be repaired by the supplier for the warranty period and then by the school's normal repair arrangements but the member of staff is responsible for transporting the equipment to and from school repair.

## Care for the equipment

- The member of staff agrees to take all reasonable care of the equipment including carrying out normal software or hardware maintenance activities, such as cleaning the device, running software updates when instructed, monitoring faults and errors and reporting errors as soon as possible to the Computing Leader.

## Acknowledgement

- I acknowledge that I have read and understood the above term and conditions.  I accept that a breach of the Acceptable Use of this equipment may lead to disciplinary action, up to and including dismissal.  Criminal proceedings will be actioned if necessary.  I also accept that a charge may be levied against me if I do not comply with this agreement and, as a consequence, repairs need to be made to the device.

**Staff Member Name (please print)**:…………………………………………………………..

**Username (Logon):**………………………………………………………………………..

**Device Description including Make and Model:**………………………………………..

**Device Serial Number:**……………………………………………………………………

**I agree that this device is:** **PASSWORD PROTECTED**
**TIMELOCKED**
**ENCRYPTED**
**HAS AN OPENING SCREEN AGREEMENT**

**Staff Member's Signature:**………………………………………………………………

**Date:**…………………………………………

**Agreement of Parties**

The school agrees to the long-term loan of the device and additional equipment to the member of staff named above.

**Headteacher's Signature:**…………………………………. **Date:**………………………