




West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

WJPS Online Safety & Acceptable Use Policy – 2024/25

KEY PEOPLE AND DATES

 <p>West Jesmond Primary School</p>	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Designated Safeguarding Lead Mark Dinsley – Deputy Headteacher 0191 281 0000 mdinsley@westjesmond.newcastle.sch.uk
	Deputy Designated Safeguarding Leads / DSL Team Members	Matt Ward – Headteacher Katharine Peggs – Assistant Headteacher Helen Sykes – Assistant Headteacher Sarah Matthews - Assistant Headteacher Gemma Jordan – SENCO Verity Groot – Bilingual and EAL Lead Liz Thompson – Early Years Lead Rachael Spanner – Out of School Club Deborah Malone – Out of School Club
	Link governor for safeguarding	Co-Chair of Governors Jane Edminson Via the school office: 0191 281 0000 jane.edminson@newcastle.gov.uk
	Curriculum leads with relevance to online safeguarding and their role	Alex Mackellar – Y6 Teacher & Computing Lead Laura Ward – PSHE Lead Carrie Young – PSHE Lead
	Network manager / other technical support	Newcastle City Council: Nick Barker / Paul Blackburn / Andy Kain IT Services - ictservicedesk@newcastle.gov.uk
	Date this policy was reviewed and by whom	January 2025 Mark Dinsley & Alex MacKellar
	Date of next review and by whom	January 2026 Mark Dinsley Alex MacKellar



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

SCOPE

This policy applies to:

- All staff users of the school network including all information systems accessed through it; this includes but is not limited to employees, contractors, consultants, external auditors, trainee teachers and temporary/casual staff, including those from private Supply Agencies;
- All children who use the school network, including access to the internet and online resources;
- All other users of the school network, for example visitors who are granted access;
- All the school's information whether held on paper or electronically, and computing equipment, including (but not limited to) computers, servers, iPads, printers, telephones, cameras and handheld devices such as tablets and smart phones;
- All school owned computing assets including but not limited to laptops, desk tops, iPads and mobile devices;
- All the school's data and all reports derived from such data;
- All programs developed by school employees or on behalf of the school, using school equipment or personal computers used for home working by school employees;
- All communication lines, and all associated equipment or devices used on school premises or connected to school resources that are capable of processing or storing the school's information; this includes all electronic devices used in school whether belonging to the school or personal devices owned by individuals;

AIMS

The aims of this policy are to ensure that:

- We have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- We 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;
- We establish clear mechanisms to identify, intervene and escalate an incident, where appropriate;



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

- All information and information systems on which the school depends are adequately protected to the appropriate level. This includes the IT infrastructure for the retrieval, sharing and dissemination of business critical data and conducting daily transactions;
- All staff and other users are aware of their responsibilities for processing personal information under the Data Protection Act 2018;
- All adult users are aware of their accountability;
- Information assets, computers and communication systems that are owned by the school and supported by IT Services are protected against external and internal threats;

West Jesmond Primary School can receive support in implementing this policy from IT Services at the Local Authority, GEM Education and HR Services at the Local Authority; these services are committed to supporting the protection of the security of the school through the preservation of:

Confidentiality – protecting information from unauthorised access and disclosure.

Integrity – safeguarding the accuracy and completeness of information and processing methods.

Availability – ensuring that information and associated services are only available to authorised users when required.

New technologies are integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone.

These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools;



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

- Education for a connected world;
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff;
- 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 2011, 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 cyberbullying 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.

RELATIONSHIPS WITH OTHER POLICIES AND PROCEDURES

Please also refer to:

- WJPS Safeguarding and child protection policy;
- WJPS Child Safeguarding Policy (policy written for children);
- WJPS Positive Behaviour and Relationships Policy;
- WJPS Behaviour Principles;
- WJPS Anti-Bullying Policy;
- WJPS Families, Relationships and Health Education Policy;
- WJPS Whistle-blowing Policy;
- WJPS Code of Conduct (for staff);
- WJPS Managing Low-Level Concerns in relation to staff conduct policy;
- Disciplinary procedure: schools must follow their disciplinary procedure where it is appropriate to take such action against an employee;
- WJPS Data Protection Policy;
- WJPS Information Security Policy.

ROLES AND RESPONSIBILITIES

All staff should make themselves aware of the contents of this policy and follow it.

The Governing Body has overall responsibility to ensure that the procedure is properly and fairly applied.



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

The Headteacher and Designated Safeguarding Lead is responsible for ensuring that all staff are aware of this policy and comply with the guidance.

Working under the direction of the Headteacher, **the Computing Subject Leader** is involved in designing and implementing the computing curriculum which effectively prepares pupils and empowers them to keep themselves safe.

The staff outlined above will monitor the implementation of this policy and review its effectiveness annually.

The experiences and requirements of the various user groups are different, so this policy is initially divided into three sections. Part A refers to staff users, Part B refers to children at the school, and Part C refers to governors, parents and other visitors. Part D concerns the managing of online safety.

PART A – STAFF USES OF SCHOOL NETWORK AND IT EQUIPMENT

Staff members represent a key component in the delivery of information security and a secure environment. Investment in secure technology and secure processes is meaningless unless all staff are aware of the role they need to play in security and what is acceptable.

Online safety is a whole school issue. The following section outlines areas of personal responsibility for staff members and is intended to provide clear guidance as to the expected role of school staff in providing and maintaining a secure IT/Computing environment in the school. IT Support from the LA and GEM Education are available to work with the school and individual staff members to provide any clarification, training or support required to ensure that everyone understands their roles and responsibilities.

A1.1 Online Safety Awareness and Training

In order to ensure that staff members fulfil their responsibility for IT and Information Security it is essential that appropriate training is provided to ensure an awareness of the legal and procedural expectations placed upon them. To this end, the school will provide training to all existing staff and to all new members of staff in the form of induction training. A 'refresher' session will be held annually.

This training will cover the following key areas:

- Known threats, risks and implications;
- Acceptable Use;
- Password Guidance;
- All staff members will be trained and made aware of their personal responsibility for maintaining information security and their roles in the classification process;



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

- Awareness of this document and any other relevant school policy documents.

A1.2 Acceptable Use

This section is intended to provide staff members with guidance on acceptable and unacceptable use when using information and the computing facilities provided by school and supported IT services. If there are any questions or concerns, advice can be sought from the Local Authority and other school advisors. The school's Senior Leadership Team may be contacted in the first instance if appropriate.

A1.3 Investigations

If there are any concerns that the policies or guidance within this document have been breached, or there is a suspicion of criminal activity then this must be reported directly to a member of the school's Senior Leadership Team or one of the school's Designated Safeguarding Leads. They will then communicate directly with the Senior Management of IT Services at the Local Authority and Human Resources to discuss any investigation that may be required. Further specialist advice may be sought from other relevant services within the Local Authority, eg the LADO.

Breaches of this policy may also result in disciplinary, civil or criminal action. Staff should be aware that school is legally obliged to report any illegal activity which takes place on the school premises or using school equipment to the Police.

A1.4 Using Computing Equipment

Each user is responsible for the equipment that they use, the data it holds and the output produced. This also applies to portable equipment, media or data that is used away from the normal place of work.

Staff – MUST
<ul style="list-style-type: none">• Keep any portable equipment securely, and carry it safely.
<ul style="list-style-type: none">• Keep log on details for resources such as Office 365 and CPOMS safe at all times and report their loss immediately.
<ul style="list-style-type: none">• Unless instructed otherwise, log off from the network every night and fully shut down the PC/Laptop.
<ul style="list-style-type: none">• Lock computer/laptop screens when you leave the room, even if you will only be away from the room for a short period of time.
<ul style="list-style-type: none">• Connect laptops to the network as often as possible to keep the anti-virus and patching protection up to date.
<ul style="list-style-type: none">• Report any problems as soon as possible to IT Services – by placing details on the IT log - including the loss of, or damage to, any computing equipment.
<ul style="list-style-type: none">• Ensure that any redundant computing equipment is disposed of in a secure and legal manner; the IT technician, working with office staff, will organise this process as the equipment needs to be



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

disposed of appropriately and removed from the school’s equipment list. IT Services will provide support in this process.
<ul style="list-style-type: none"> • Ensure that all software used is correctly licensed and covered by a school or Local Authority license (i.e. not home or personal user). The licence terms for free software must be carefully examined to ensure it meets these requirements.
<ul style="list-style-type: none"> • Ensure all software is installed by IT Services (Local Authority).
<ul style="list-style-type: none"> • Only take photographs that are for school purposes using school equipment.
<ul style="list-style-type: none"> • Ensure permission has been given by parents before using photographs of children on the school website. (Check permissions saved on the school network.)

Staff - MUST NOT
<ul style="list-style-type: none"> • Allow supply staff or visitors, to use a machine logged on using your or another person’s username and password, except when closely supervised e.g. children using the Smartboard with a teacher’s laptop attached in a lesson.
<ul style="list-style-type: none"> • Save any information on to any computer or device which is not registered as school equipment.
<ul style="list-style-type: none"> • Use personal cameras including mobile phones to take photographs of children from school without prior consent from the Headteacher. In this instance, staff must delete photographs from devices (from camera roll and ‘recently deleted’) on the same day and before leaving the building.

Staff – SHOULD
<ul style="list-style-type: none"> • Lock your PC/Laptop screen (using Ctrl/Alt/Del then ‘Lock Computer’) whenever you are away from your desk, to prevent someone accidentally or deliberately looking at information, making unauthorised changes, or sending emails in your name.
<ul style="list-style-type: none"> • Shut down or logout if you are going to be away from your machine for any length of time.
<ul style="list-style-type: none"> • Report any instances of possible security breaches, including near misses. For example, if: A colleague is using someone else’s log-in name and password OR You can see personal information on a computer screen in an unattended area.

A1.5 Passwords

Effective username and password combinations are a basic security requirement for any information system. But they are only effective if used properly.

Staff – MUST
Choose a password that: <ul style="list-style-type: none"> • Is at least 8 characters long. • Contains at least one letter and at least one numeric character. • Contains both uppercase and lowercase letters and at least one punctuation mark or other ‘special character’. • Where the system cannot meet these requirements you will use the maximum complexity that the system allows. • Change your password as soon as possible, if anyone else gets it know it.



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

Staff – MUST NOT

- Disclose your password to anyone else.
- Use another person's logon name or password or allow someone to use another person's logon name and password.
- Use another person's machine whilst they are not there if they have not locked it (log the machine off or lock it for them).
- Reply to any email asking for your username, log in details or password (even with a refusal since this lets the sender know that they have located a valid email address).

A1.6 Saving Files

Staff – SHOULD

- Save files on the server rather than on to your PC (including laptops).
- Save files to appropriate locations on the network, taking into consideration the access provided to each drive e.g. the Common drive can be accessed by all users.
- Restrict access to strictly confidential information on a need to know basis.
- Password protect any documents including confidential information

A1. 7 Using the Internet and Email facilities

All network users have access to the Internet and e-mail. By accepting your network account password and related information, and accessing the network, you agree to keep this policy. You also agree to report any network misuse to the IT Services and the School's Senior Leadership Team. Misuse includes policy violations that harm another person or an individual's property.

The school provides each member of staff with an email address. This email account should be used for work purposes only. Staff must enable multi-factor Microsoft authentication on their email account(s) to access their account outside of school. All work-related business should be conducted using the email address the school has provided.

This email account should be used for **work purposes only**. Staff must enable multi-factor Microsoft authentication on their email account(s). All work-related business should be conducted using the email address the school has provided. Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account. Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents.



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. If staff send an email in error that contains the personal information of another person, they must the Headteacher or DSL and office staff immediately and follow our data breach procedure.

A1.8 Mobile Devices including iPads and Laptops

Mobile devices include iPads, laptops and memory sticks, but this list is not exhaustive. Laptops and iPads allocated to teachers are the only type of mobile devices which should be taken off the school premises. In doing so, you must adhere to this policy. 'One Drive' (part of Office 365) or 'Any Connect' should be used to access files from the school network rather than saving them on mobile devices. In exceptional circumstances, a memory stick may be used with the approval of the Headteacher, but staff members are responsible for ensuring sensitive data, for example personal information, is NEVER saved on ANY portable device. Sensitive data includes children's names, dates of birth and addresses, but there are many other examples of sensitive data in school, if you are unsure you should talk to the Headteacher or DSL.

A1.9 Taking and Using Photographs and Videos of Children

When children join West Jesmond Primary School, parents/carers will be asked to sign a photograph permissions form to provide parental consent for the publishing of photographs of their child/children. This form covers permission until they leave school at the end of Year 6. Parents/carers sign this form to give permission and are aware that to change permission at any time they must inform the school office.

It is the responsibility of all staff to access and check this information whenever they are publishing photographs of children or their work to the internet or to the media/press.

Taking photographs and videos in school is an important source of evidence of achievement and attainment, and also helps share learning and school events with others e.g. by using them on the website, Seesaw, Tapestry, Facebook and displaying them in school. Guidance on taking photographs and videos is included in this policy for the protection of the children and staff in school.



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

- Photos and videos taken in school should be taken with a clear purpose in mind, e.g. recording an activity and achievement, and taken at an appropriate, legitimate time;
- They should only ever show the children in a positive light and be appropriate in terms of children's dress, position and behaviour.

Only school devices should be used to take photographs of pupils. There might be exceptions to this such as taking photographs on visits to use on the school's Facebook account, in these cases prior permission must be sought from the Headteacher. In this instance, once permission has been sought, staff must delete photographs from devices (from camera roll and 'recently deleted') in the presence of a witness from the SLT, on the same day and before leaving the building.

If a member of staff is concerned about the taking and/or use of photographs and videos of children in school, they **MUST** report this to a member of the school's Senior Leadership Team in order to fulfil their professional responsibilities to the children in their care. If the concern is about a member of the SLT, in particular the Headteacher, staff should report to the chair of Governors.

All staff are aware of the whistleblowing policy and what to do with concerns which are considered low level and more serious.

Photographs and videos will be used on the school website (www.westjesmondprimary.org.uk) and school and class social media accounts (eg: Weduc, Facebook, Seesaw, Tapestry, etc.) if parental permission has been given. Photographs may also be used in displays around school and newsletters. Photographs and videos on the aforementioned platforms will not be labelled with the name of the children, and photographs and videos of the children will not be used if their name is in the accompanying text. The press sometimes publish names with photographs, despite school's policy, and this is accounted for in the permission form. Photographs and videos will also be uploaded to the Seesaw app where they can be added to individual child accounts.

Tapestry will be used in Early Years to record observations which will include photographs and names of the children. Parents/Carers sign a permission form for the use of Tapestry within their school induction pack. The accounts on Tapestry, will be archived each year and monitored by the EFYS lead.

A.10 Personal Responsibility

- Access to the Internet and email during work hours shall be through a school device attached to the network;



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

- E-mail access is also permitted via the webmail portal or an authorised mobile device;
- Staff should only use approved e-mail systems within school, such as the schools exchange email to send e-mails related to school business;
- Work related information must not be communicated on non-school e-mail systems. The security of data cannot be guaranteed;
- If other staff need to access your email account (for example, during leave or sickness) you should seek help and support on this area is available through IT Services;
- A staff WhatsApp group is sometimes used to share information regarding school – this information is non-confidential and non-child related;
- No information should be sent via email which does not align with the guidance stated in the school's Information Security Policy. Most school information including children's records fall into the 'Protect' category and if these need to be sent electronically, they need to be encrypted. Should this be required, advice should be sought from IT Services. Information about 'Looked After Children' is 'Restricted' and encrypted email must also be used for this

A1.11 Personal Information

The term 'Personal information' is used frequently in e-safety training and throughout this policy. The term refers to any information that in combination identifies one person to another. This could be a name, address, National Insurance or telephone number. It could also be the type of job they do or the name and location of the school they attend.

- You should take care when sending personal information electronically, this includes uploading or sending information to an Internet site.

A1.12 The security of external communications cannot be guaranteed

Where you have an authorised business need to electronically send sensitive or confidential personal information, which relates to pupils, clients or staff, you must refer to the school's Information Security Policy. If in doubt, please consult the School Business Manager.

A1.13 Access to Office 365 including One Drive

Access to files from the school network from locations outside school is granted to teaching staff through use of One Drive, part of the Microsoft Office 365 suite. By uploading files prior to leaving the building, staff are able to access the files when away from school. This is a secure means by which this can occur, significantly more secure than using a laptop's hard



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

drive, a memory stick or an external hard drive which are vulnerable to loss and theft. It also allows access to e-mail away from school.

- Staff members who make use of Any Connect and Office 365 from school should operate to the same acceptable use standards as if they were in school. Newcastle LA have assured the school of the high level of security associated with Office 365 but files can be downloaded onto other devices and therefore school requires staff not to use Any Connect and Office 365 in this manner;
- You are personally responsible for keeping any work related data stored on any mobile equipment or on Office 365 safe and secure.

A1.14 Unacceptable Use

Any use of the internet or IT facilities which is against any relevant legislation or any internal school policies is unacceptable and could lead to disciplinary action. If you are in any doubt about any use, you should contact the school's Senior Leadership Team, DSL or IT Services.

Examples of unacceptable use include:

- Using the school's ICT facilities to breach intellectual property rights or copyright;
- Breaching the school's policies or procedures;
- Any illegal conduct, or statements which are deemed to be advocating illegal activity;
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams;
- Activity which defames or disparages the school, or risks bringing the school into disrepute;
- Sharing confidential information about the school, its pupils, or other members of the school community;
- Connecting any device to the school's ICT network without approval;
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data;
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password protected information, without approval from authorised personnel;
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities;
- Causing intentional damage to the school's ICT facilities;



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel;
- Using 'chat rooms' and 'discussion forums' of a personal, malicious or illegal nature;
- Circulating jokes, personal photographs or making malicious comments about other people on 'social networking sites';
- Any form of online harassment (or cyberbullying), including harassment by volume of communications on 'chat rooms', 'discussion forums' or 'social networking sites', or sending 'spam';
- Creating material containing false claims of a deceptive nature;
- Use for private business purposes;
- Any form of gambling;
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms;
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way; (This list is not exhaustive.)

Deliberate unlawful or inappropriate material must not be viewed, stored or distributed using the school's IT system or personal devices in school. This can include any material which is in violation of any law or regulation which can be considered by any reasonable person in its context to:

- Be defamatory;
- Be violent;
- Be offensive;
- Be abusive;
- Be indecent or obscene;
- Incite hatred;
- Constitute bullying or harassment;
- Breach anyone's confidence, privacy, trade secrets or copyright;
- Where possible, IT Services will prevent access to material known to be of an offensive or undesirable nature using security tools and filtering software;
- Smoothwall Monitor is used to alert the Headteacher and DSL to potential offensive content which may have been searched or typed;
- If you receive an email or access a website which you consider to be offensive or potentially illegal, you must report the matter to the Headteacher, DSL or IT Services;
- If you receive an email that you consider to be spam, you should forward it to ictservicedesk@newcastle.gov.uk and then future incoming e-mails from that address can be blocked.



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

A1.15 Personal Devices including mobile phones

Staff members may use personal devices e.g. phones on school premises, provided they are used outside of working time, not in the sight or presence of children, and not used with children from the school.

Personal devices can be connected to the school guest Wi-Fi network which is monitored by the Local Authority and IT Services. Personal devices are for personal use only and all use of personal devices must comply with this policy when used in school. When on the school site and using your own mobile phone you must comply with all aspects of Acceptable Use as stated in this policy.

Mobile phones should not be used as part of classroom practice. They should be stored out of sight of children, e.g. in a bag or drawer; they SHOULD NOT be kept on a teacher's desk whilst children are in the classroom. Staff are not allowed to use their mobile phone to take photographs or videos of children in school for any purpose, other than in exceptional circumstances or with prior permission from the Headteacher.

A1.16 Social Networking

Staff members may use Social Networking sites such as Facebook, Instagram and X for either personal or professional reasons. Forming a Personal Learning Network via social networking sites can lead to significant benefits for their Continuing Professional Development (eg: Task Design on Facebook). However, when using sites such as X and Facebook, staff members MUST be aware of the language they use and the comments they make and ensure they maintain professional in relation to the teachers standards.

Privacy settings are not infallible and care should be taken by members of staff to protect their professionalism. The potential audience (e.g. children at the school and their parents, employers etc.) must be considered. It is recommended that comments are not made that would not normally be shared publicly with these groups.

Staff members should not allow access to their own personal areas or open lines of communication with children or parents via social networking sites. It is very important that staff members maintain professional relationships with children or parents at any time and this would be compromised by allowing children access to personal information or photographs.

Use of Social Networking sites for school business (e.g. sharing information with parents, promoting the school etc.) must be through use of a school account e.g. Facebook.

A1.17 Generative Artificial Intelligence (AI)



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age. Through the Digital Citizenship aspects of the Computing curriculum, the school will teach pupils to be discerning with healthy scepticism.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

Microsoft Co-Pilot is utilised within the local authority's filtering systems. This is the AI tool which staff will use within the school setting and on school devices.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

A2 Monitoring

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. IT Services will, if requested, facilitate the monitoring of Internet and E-mail facilities and their usage, on behalf of the school to highlight non-compliance. This monitoring will include, but will not be limited to:

- All internet sites staff browse on or through the school network;
- All transactions staff make via the internet on the school network;
- All files downloaded or uploaded to or from the internet on the school network;
- All e-mails sent and received;
- All attachments sent and received;

Therefore staff should not expect privacy on any e-mails that are sent or received, or websites visited.

Logs are retained on all emails that are sent and received as well as all websites that have been browsed by any user. IT Services may be required to disclose any information kept on



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

computer systems to outside parties or law enforcement authorities. This would always happen in consultation with the school's Senior Leadership Team.

A3 Sanctions

Failure to comply with any of the requirements of this policy may result in further action being taken by the school in line with the appropriate disciplinary policy. Instances of non-compliance with this policy shall be identified, documented and escalated. Remedial measures shall be implemented by IT Services and school's Senior Leadership Team as quickly as possible. Deliberate non-compliance by individuals, whether they are system administrators or other users, shall be treated as a disciplinary offence, and may also result in civil or criminal action being taken.

Violations of established security procedures and inadvertent and deliberate compromise of School proprietary and personal information are actions that are adverse to the security of a school and as such may warrant disciplinary, civil or criminal action, based on the severity of the incident.

Some breaches of this policy may result in loss of data such as personal information, and this must be reported to the Information Commissioner's Office. The loss is publicly declared and the loss of equipment and/or data must be explained, with the school being held responsible.

PART B – CHILDREN USING THE SCHOOL NETWORK AND IT EQUIPMENT

B1 Guidance

This part of the policy outlines the school's purpose in providing an IT network (including internet access and email facilities) for children at West Jesmond Primary School. It also explains how the school seeks to avoid the potential problems that unrestricted Internet access could give rise to. The policy applies to all children who are pupils at West Jesmond Primary School, but also applies to members of staff when using the internet with the children.

B2 Internet Access in School

Providing access to the Internet in school raises educational standards and enhances learning opportunities. Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

them, appropriate to their age and stage (Education for a Connected World 2020). All PCs, laptops and iPads in school have internet access and children will use the internet to complete tasks related to their work in a range of curriculum areas. Laptops and iPads are available to children only under the supervision of staff. This includes the use of specialist ICT equipment, such as that used for music or design and technology.

B3 Ensuring Internet Access is safe and appropriate – Online Safety

The internet, as a communications medium, is available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by teachers, and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our internet access provides a service designed for children including a web filtering system (Smoothwall Filter) intended to prevent access to material inappropriate for them;
- We also use the Smoothwall Monitor system to alert the Headteacher and DSL to any inappropriate behaviour from children working on online devices;
- Children using the internet will be working in the classroom or other learning environment, during lesson time and will be supervised by an adult (usually the class teacher) at all times. Class teachers have access to 'Classroom Manager' to check the work children are completing on their iPads;
- Staff will check that the sites pre-selected for use by the children are appropriate to the age and maturity of pupils;
- Staff will be particularly vigilant when children are undertaking their own search and will check that they are following the agreed search plan;
- Children will be taught to use 'the internet' in all its forms responsibly in order to reduce the risk to themselves and others through our robust computing and PSHE curriculum;
- Our school rules (the 'Pupil Use Agreement' – see appendix A) will be posted in every classroom, taught to children at the beginning of the school year, and then revisited at appropriate points throughout the year;
- Teachers are able to use software such as Classroom Manager when using school iPads, to quickly and effectively monitor searches and apps that children are using;



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

- Methods to quantify and minimise the risk of children being exposed to inappropriate material will be reviewed when developments occur and advice from the Local Authority, our Internet Service Provider and the DFE will be sought;
- It is the experience here and in other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. **Neither the school nor Newcastle LA can accept liability for the material accessed, or any consequences thereof.**

In the unlikely event that an incident in which a child is exposed to offensive or upsetting material occurs, the school will respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children will be taken by the Headteacher or DSL and the child's class teacher. All teaching staff will be made aware of the incident if appropriate.

In the unlikely event that one or more pupils discover (view) inappropriate material, the first priority will be to give them appropriate support. The children's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and children to resolve any issue. If staff or children discover unsuitable sites the Headteacher or DSL will be informed and the incident will be logged. The Headteacher or DSL will report the URL (address) and content to IT Services and seek advice from them; if it is thought that the material is illegal, after consultation with IT Services, the site will be referred to the Police.

The children are expected to play their part in reducing the risk of viewing inappropriate material by obeying the rules within the 'Pupil Use Agreement', which have been designed to help protect them from exposure to internet sites carrying offensive material.

The Headteacher, DSL and class teachers have the responsibility for logging safeguarding issues related to online safety on CPOMS.

B4 Using the internet as part of the school curriculum

As part of the Computing curriculum, pupils will learn how to use a web browser and suitable web search engines so they can access the internet to find and evaluate information. Access to the internet will be a planned part of the curriculum that will enrich and extend learning activities and will be integrated into long-term and short-term planning.

As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for internet use. When accessing the internet on iPads, children



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

will only be able to access through the Smoothwall app. This ensures that appropriate filtering and monitoring systems are in place.

Note: For the purpose of Y6 tutoring sessions, the Safari browser will be used as the software isn't supported by the Smoothwall app. The Safari app has been time blocked meaning it can be only be accessed during this tutoring time on a specific iPad set.

Different ways of accessing information from the internet will be used depending upon the nature of the material being accessed:

- access to the internet may be by teacher demonstration;
- children may be given a suitable web page or a single web site to access (Children can be locked into this on iPads);
- children may be provided with lists of relevant and suitable web sites which they may access;
- more experienced children may be allowed to undertake their own internet search having agreed a search plan with their teacher; pupils will be expected to observe the rules within the 'Pupil Use Agreement' and will be informed that checks can and will be made on the sites they access – through Classroom Manager.

Children accessing the internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the internet once they have been taught the within the 'Pupil Use Agreement' and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the internet.

B4 Using information from the internet

We believe that, in order to use information from the internet effectively, it is important for children to develop an understanding of the nature of the internet and the information available on it. These Digital Literacy skills are important for the children now, but are also life skills which are important for the children's future. Through our school Computing curriculum children will learn about the three main strands of the Computing curriculum; Computer Science, Digital Literacy and Digital Citizenship, and develop an understanding of the nature and purpose of their digital world and how it affects their lives.

- Teachers will explicitly teach 'Digital Citizenship' through the use of Project Evolve, ensuring that children are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium);



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

- When copying materials from the Web, children will be taught to observe copyright protections (copyright and ownership strand Project Evolve);
- Where appropriate children will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed (Privacy and Security strand Project Evolve).

B8 Use of iPads and Apps

Children in school will have access to iPads which have a range of appropriate, educational apps on to support learning. Each class in school will have their own Seesaw account which will be accessible through staff and children's iPads.

Through the schools Computing Curriculum, children will be taught how to upload photographs from the iPad to Seesaw and take photographs/videos on the app. The class teacher will have responsibility for checking work which the children post and giving feedback on this.

B9 Sanctions

If the privileges of access to the internet and school IT Equipment are abused by failing to follow the rules that have been taught, then sanctions consistent with our Behaviour and Relationships Policy (refer to Behaviour and Relationship policy) will be applied. This may involve informing the parents/carers.

Teachers may also consider whether access to IT facilities in school may be denied for a period.

PART C – GOVERNORS, VISITORS AND PARENTS USING THE SCHOOL NETWORK AND IT EQUIPMENT

C1 Access to the school network for Governors, Parents and Visitors

Governors, parents and other visitors (including supply staff) to school may need access to the school network. For example a visiting speaker may need to show a presentation on a Smartboard or use a website, a Governor may use a school PC to complete a task related to their role, or a parent helper may be making resources while helping in school. For this reason, a 'supply' and 'guest' account has been set up with appropriate access permissions. If use of the school network is needed, the Governor, parent or visitor will be asked to read section A1.4 of this policy, with a full version being available on request, and if they agree to adhere to it, they will be given a user name and password.



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

C2 Access to the school network for Trainee/Student Teachers

The school often hosts trainee or student teachers on placements which form part of their Initial Teacher Training (ITT). Trainee or student teachers require access to the school network as part of their teaching commitments and to complete their professional studies. Each long term trainee will be given an individual user name and password to enable them to access the school network and the internet. The account will also provide access to a network drive where they may save files. As well as subject to the monitoring described in Part A, the network drive provided will also be accessible to the Headteacher and DSL for monitoring purposes.

C3 Working with children and PCs/laptops/iPads

If Governors, parents or other visitors are working with children using computers or iPads, particularly if they are using the internet, they should be made aware of the importance of e-safety and the rules children follow. If they become aware of children viewing any inappropriate content, they MUST inform the member of staff they are working with or the Headteacher or DSL.

C4 Taking photographs

Visitors to school may not take photographs of the children without first requesting and receiving permission from the Headteacher. Unless the Headteacher decides differently, permission is given for parents to take photographs and record videos of children performing in class assemblies, the Year 6 leavers' assembly, Christmas concerts and any other performances; this is on the understanding that these are for personal use only. Visitors will be told this very clearly in advance. Parents and carers have been told to inform school if they do not want their children to be included.

C5 Sanctions

While not subject to disciplinary procedures due to the nature of their role, any visitors who breach this policy may be subject to civil or criminal action, and they should be aware that school is obliged to report illegal activity taking place on school premises or using school equipment to the Police.

C6 Educating Parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the 'Pupil Use Agreement' at the beginning of each academic year (beginning September 2025)



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming;
- Exposure to radicalising content;
- Sharing of indecent imagery of pupils, e.g. sexting;
- Cyberbullying;
- Exposure to age-inappropriate content, e.g. pornography;
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Weduc communications;
- GEM Education parent workshops;
- Newsletters;
- Online resources – eg: parental guides.

PART D – MANAGING ONLINE SAFETY

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Headteacher and DSL have overall responsibility for the school's approach to online safety, with support from other DSLs and the Computing Subject Lead, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the Local Authority, Clennell Education Solutions, police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

- Staff and governors receive regular training;
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation;
- Online safety is integrated into learning throughout the curriculum;
- Children access assemblies concerns online safety.

Handling Online Safety Concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the Headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and ICT technicians, and



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL on CPOMS.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages;
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras;
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible;
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name;
- Unpleasant messages sent via instant messaging;
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook;
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse;
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Antibullying Policy.



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence;
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks;
- Sexualised online bullying, e.g. sexual jokes or taunts;
- Unwanted and unsolicited sexual comments and messages;
- Consensual or non-consensual sharing of sexualised imagery;
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse.

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Safeguarding and Child Protection policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online;
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met;
- Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an “online hoax” is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, “harmful online challenges” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes;
- Careful to avoid needlessly scaring or distressing pupils;
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils;
- Proportional to the actual or perceived risk;
- Helpful to the pupils who are, or are perceived to be, at risk;
- Appropriate for the relevant pupils' age and developmental stage;
- Supportive;
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

MONITORING AND REVIEW

The policy will be reviewed on an annual basis by the relevant staff (Headteacher, DSL, Computing Lead and Governors) to ensure it is appropriate in light of recommended best practice and complies with statutory regulations. In the event of any conflict with statutory regulations, the legal provisions will have precedence over this procedure in all cases. The Headteacher and DSL, reporting to the Governing Body, will monitor the application of this policy and procedure, particularly to ensure that the school's practices comply with it.



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

Revision Record of Published Versions			
Author	Creation Date	Version	Status
West Jesmond Primary	8 th January 2013	1.0	Drafted by D.Martin DHT
Changed by	Revision Date	Version	Status
West Jesmond Primary	22 nd January 2014	2.0	Annual Review and update D.Martin DHT
West Jesmond Primary	4 th February 2014	3.0	Annual Review by Governors
West Jesmond Primary	26 th February 2016	4.0	Review and update D.Martin HS
West Jesmond Primary	6 th December 2016	4.0	Review and update AHT (TJ)
West Jesmond Primary	Review due September 2019	4.0	3 yearly review
West Jesmond Primary	30/1/2019	4.1	Reviewed – next update 30/1/2022 update reflects GDPR regulations
West Jesmond Primary	14/10/19	4.2	Review and update by TJ (AHT)
Changed by	Revision Date	Version	Status
West Jesmond Primary	March 2025	5.0	Policy changed and updated to reflect trends in online safety – MD (DHT)



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

Appendix A – KS1 & KS2 ‘Pupil Use Agreement’ Documents:

**WJPS – Online Safety
Pupil Use Agreement for KS1**

This is how I stay safe when I use digital devices:

- I know that my teacher can check what I do online and that if I break the rules I might not be allowed to use a digital device.
- I will always use the correct numbered device that has been given to me.
- I will only share my password with my teacher.
- I will only use the device for things my teacher has told me to.
- I will make sure that all the messages I send are polite.
- I will tell a teacher if I see something that makes me feel scared or uncomfortable on the screen.
- I will not reply to any nasty message or anything that makes me feel uncomfortable.
- I will not tell people about myself online (I will not tell them my name, mobile phone number, anything about my home, family, pets and school).
- I will never agree to meet a stranger.
- I will not put photographs of myself online without asking a teacher.
- I will always follow the West Jesmond Way when I’m online.

Signed _____





West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone.

These technologies can stimulate discussion, promote creativity and raise awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Pupil Use Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. The school will try to ensure that pupils will have appropriate access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Parent / Carer Signature

As the parent/carers, I understand that the school has discussed the Pupil Use Agreement with my son/daughter as part of whole school commitment to Digital Citizenship both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet. I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of this Pupil Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Name of Pupil _____

Class _____

Signed (parent/carers) _____

Date _____



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

WJPS – Online Safety Pupil Use Agreement for KS2

At school we use digital devices, and other resources connected to the internet and our wireless network. These rules will keep us safe and help us to be fair to others:

- I understand that teachers check my computer files and will monitor the Internet sites I visit – including anything I type, produce or search.
- I will always use the correct numbered device that has been assigned to me.
- I will keep my passwords for logging in to any device or application to myself – if I think others know my passwords I shall tell my teacher.
- I shall use the online activities and sites which school allows me to access from home appropriately.
- I will not use my own mobile device/phone/smart-watch in school and will hand it to my class teacher at the start of the day.
- If the device asks for an update, I shall check this with my teacher.
- I will only use devices for things my teacher has told me to.
- I will not use the internet to access unsuitable material.
- The messages I send will be polite and respectful.
- I will always report anything that I feel is unkind or makes me feel unsafe or uncomfortable to my teacher. I will not reply to any nasty messages.
- I will always keep my personal details private (e.g my name, mobile phone number, family information, journey to school, pets, hobbies).
- I will not register my details with online activities and websites without the permission of my teacher.
- I will not share files or photos without the permission of my teacher – including the use of air drop.
- I will not copy text or pictures from the internet and pretend it is my own work.
- I will treat computer equipment, like all school equipment, with care and respect.
- I know that if I break the rules I might not be allowed to use a digital device.
- I will always follow the West Jesmond Way when I'm online.

Signed _____



West Jesmond Primary School:

Online Safety & Acceptable Use Policy - 2024/5

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone.

These technologies can stimulate discussion, promote creativity and raise awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Pupil Use Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. The school will try to ensure that pupils will have appropriate access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Parent / Carer Signature

As the parent/carers, I understand that the school has discussed the Pupil Use Agreement with my son/daughter as part of whole school commitment to Digital Citizenship both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet. I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of this Pupil Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Name of Pupil _____

Class _____

Signed (parent/carers) _____

Date _____