Western
Primary School
CREATING SUCCESS STORIES

E-Safety and Acceptable Use Policy

Reviewed: March 2019
Next Review: March 2022

For clarity, this policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, children and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents.

The School's Vision

At Western Primary School we seek to develop in our children a love of learning that will last a lifetime. We are committed to providing a stimulating environment, combining high standards and a broad, rich curriculum with the understanding that every child approaches learning in a unique way. In a happy and safe atmosphere, our children have the freedom to engage and discover with a focused and experienced team supporting every child in striving to meet and exceed their personal goals. Educating our children with a fusion of excellence and enjoyment, Western Primary School is privileged to be part of this crucial stage of childhood, encouraging our children in creating their own success stories.
The principles of the EYFS underpin teaching and learning in the Early Years department of the school. The children experience a range of activities in all areas of provision which cater for the needs of all pupils.

Rationale

We recognise the Internet as being an integral part of teaching and learning. The Internet can raise educational standards by offering pupils and teachers opportunities to search for information from a wide range of sources and to enhance the child's knowledge of the outside world.

As well as providing many benefits and new opportunities, the use of ICT, and the Internet in particular, may lead to safety issues for the children. We accept that this must be managed in order to protect the children.

Safeguarding is a serious matter; at Western Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the child or liability to the school.

This policy is available for anybody to read on the Western Primary School website; upon review all members of staff will sign as read and understood, both the e-safety policy and the Staff Acceptable Use Policy.

Aims

At Western we believe it is very important to:

- Educate children to help them to develop a safe, responsible and mature attitude towards Internet use, inside and outside the school environment,
- Regulate Internet access to ensure children are using websites and materials that are appropriate to them,
- All staff to monitor children's access to the Internet both in class and in lunch time clubs,
- Establish home school agreements, involving parents and children and staff about acceptable use of the Internet.

Internet use will support, extend and enhance learning:

- Children will be given clear objectives for Internet use,
- Web content will be subject to age-appropriate filters,
- Internet use will be embedded in the curriculum.

Children will develop an understanding of the uses, importance and limitations of the Internet E-Safety Policy:

- Children will be taught how to effectively use the Internet for research purposes,
- Children will be taught to evaluate information on the Internet,
- Children will be taught how to report inappropriate web content through the use the CEOP button.

Children will develop a positive attitude to the Internet and develop their ICT capability through both independent and collaborative working:

- Children will use the Internet to enhance their learning experience,
- Children have opportunities to engage in independent and collaborative learning using the Internet and other digital technologies.

Children will use existing technologies safely:

- Children will be taught about e-safety through planned lessons and resources from CEOP,
- Children will be made aware of how to use the CEOP button.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:

  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. children, all staff, governing body and parents.
- All e-safety incidents are dealt with promptly and appropriately.

E-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to the Striving Success Group Leader.

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst being familiar with the latest research and available resources for school and home use.
- Review this policy regularly.
- Advise the governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function;

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure
- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer/ Headteacher.
- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

All Users

All users are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer/Headteacher (and an e-Safety Incident report is made). If you are unsure the matter is to be raised with the e-Safety Officer/Headteacher to make a decision.

All Children

The boundaries of use of ICT equipment and services in this school are given in the children's Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

e-Safety is embedded into our curriculum; children will be given the appropriate advice and guidance by staff. Similarly all children will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters, the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that children are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the children's Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

At Western Primary School we use a range of devices including PC's, laptops and Apple ipads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use North Yorkshire software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data as defined by GDPR are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does not mean password protected.)*

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least fortnightly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; children upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos –All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Western Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Western Primary School in the future and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer for a decision to be made. Any new service will be risk assessed

before use is permitted.

- Kidsblog – used by staff and children in KS2.
- Classlist – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community.

In addition, the following is to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded.
- There is to be no identification of children using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use.

Prevent

In order to fulfil the Prevent duty, it is essential that staff are able to identify children who may be vulnerable to radicalisation, and know what to do when they are identified. Protecting children from the risk of radicalisation is seen as part of schools' wider safeguarding duties, and is similar in nature to protecting children from other harms (e.g. drugs, gangs, neglect, sexual exploitation), whether these come from within their family or are the product of outside influences. For further information refer to RKLT Safeguarding and child Protection Policy.

Notice and take down policy

Should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer by a CPOMS incident. The e-Safety Officer will assist in taking the appropriate action to deal with the incident.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Western Primary School will have an annual programme of training which is suitable to the audience.

e-Safety for children is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the child's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the E-Safety and Acceptable Use Policy. Once you have read and understood both you must sign this policy sheet.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e- safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

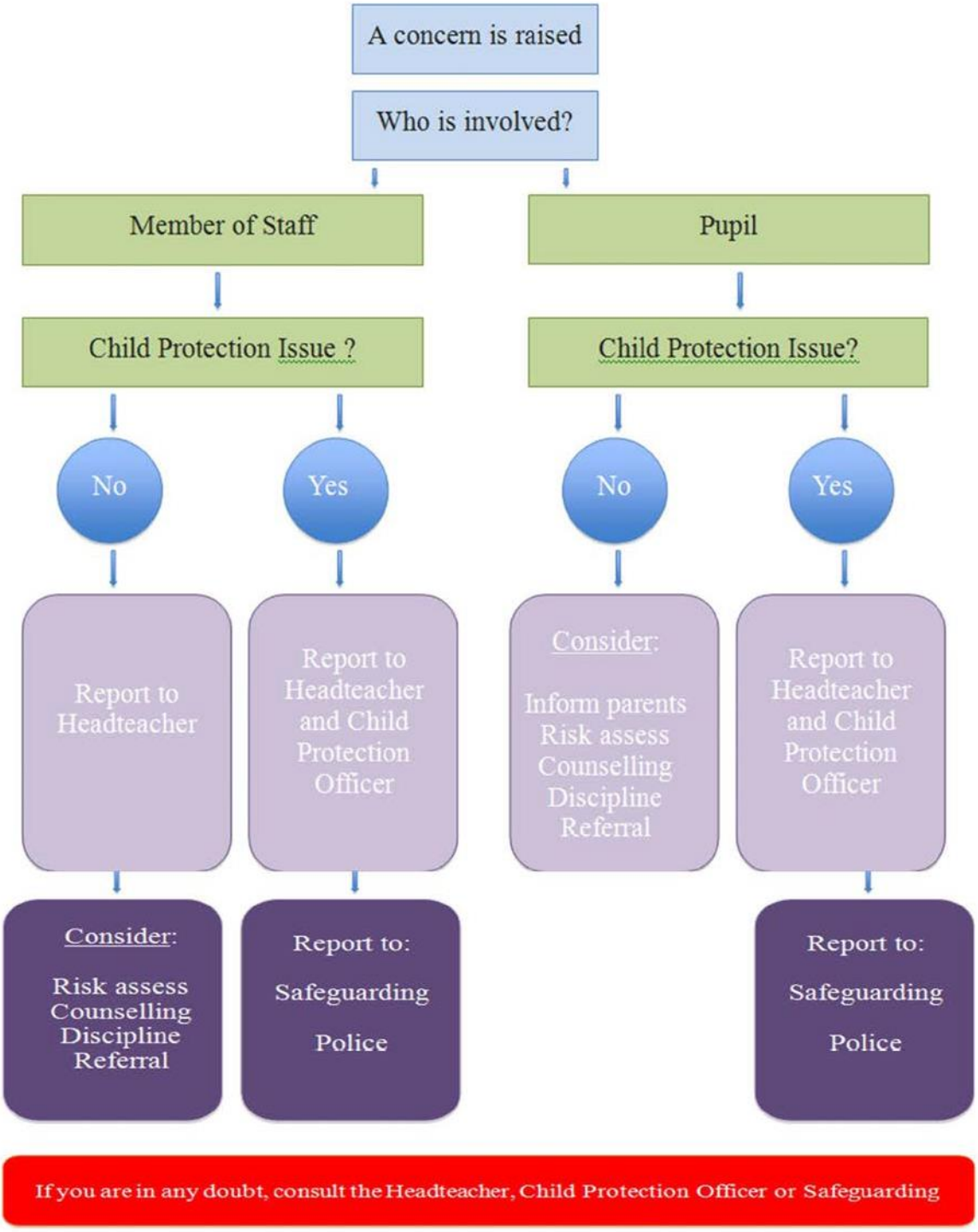
Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the Easi-PC Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with children.

NAME :

SIGNATURE :


A concern is raised
Who is involved?
Member of Staff
Pupil
Child Protection Issue ?
Child Protection Issue?
No
Yes
No
Yes
Report to Headteacher
Report to Headteacher and Child Protection Officer
Consider:
Inform parents
Risk assess
Counselling
Discipline
Referral
Report to Headteacher and Child Protection Officer
Consider:
Risk assess
Counselling
Discipline
Referral
Report to:
Safeguarding
Police
Report to:
Safeguarding
Police
If you are in any doubt, consult the Headteacher, Child Protection Officer or Safeguarding