WESTFIELD SCHOOL POLICY AND PROCEDURE

E-safety Policy

PRINCIPAL AUTHOR: S Eades, Nicki Gilbert

Latest Date revised: August 2024

WESTFIELD SCHOOL

POLICY DOCUMENT

E-SAFETY POLICY

Rationale

Westfield School aims to provide access to the range of teaching and learning opportunities provided by the internet and the technologies we use in everyday life whilst minimising the risk of any harm. The school manages the issue of e-safety as part of its overall commitment to the safeguarding and wellbeing of pupils.

AIMS

- To help pupils to keep themselves safe online, encouraging pupils to adopt safe and responsible practices and deal sensibly with risk when using the internet.
- To provide all pupils and students with a stimulating, challenging and supportive learning environment;
- To develop independence and key skills
- To instil core values
- To promote the spiritual, moral, cultural, mental and physical development of pupils and students;
- To prepare pupils for the opportunities, responsibilities and experiences of adult life;

Introduction:

The use of new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Un-authorised access to / loss of / sharing of, personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, peer on peer and child protection policies).
It is impossible to eliminate risks completely; it is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.
ICT in the 21st Century is seen as an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. Consequently,

schools need to build in the use of these technologies in order to arm young people with the skills to access life-long learning and employment.
Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Search engines
- Websites
- Email
- Approved Social Networking
- Blogs and Wikis
- Podcasting
- Digital Video
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. At Westfield School, we understand the responsibility to educate our pupils on E Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, smart phones, and portable media players, etc.).

Objectives:

- Students and staff should be able to use the internet and technologies identified within this policy to enhance their teaching and learning.
- Students and staff should be taught a set of safe and responsible behaviours in order to help keep them safe on the internet.
- Students and staff should be taught principles of E safety to help safeguard them both within and outside of school.
- Parents and carers should be informed of the potential dangers of the internet and its associated technologies, and they should be supported by the school to take measures to ensure safe usage by all.

Responsibilities

Responsibilities of the school as a whole

We believe that E Safety is the responsibility of the whole school, and everyone has their part to play in ensuring all members are able to benefit from the opportunities that technology provides for teaching and learning. The following responsibilities are examples of key roles everyone has to play here at Westfield:

Responsibilities of the Head Teacher/Senior Leadership Team/DSL

- The Headteacher is responsible for the implementation and effectiveness of this policy and for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.
- Develop and promote an E Safety culture within school and ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- Make appropriate resources, training and support available to ensure staff are able to carry out their roles with regard to E Safety effectively.
- Take ultimate responsibility for the E Safety of the school.
- Be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See Managing Allegations against a member of staff policy/guidance)
- Liaise with the local authority, Herefordshire safeguarding partners and other relevant agencies.
- Ensure that E Safety is promoted by parents and carers.

Responsibilities of Designated Safeguarding Leads

- Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Report to the School Safeguarding Governor serious breaches of the E-Safety Policy or data breaches.
- Provide training and advice for staff.
- Liaises with the Local Authority and our named ICT support.
- Receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Are trained in and share with staff an awareness and understanding of e-safety issues and the potential for serious child protection issues that can arise from:

  - Sharing of personal data
  - Access to illegal / inappropriate materials
  - Inappropriate on-line contact with adults / strangers
  - Potential or actual incidents of grooming
  - Cyber-bullying/ peer on peer abuse
  - Sexting
  - Revenge pornography/ up skirting
  - Radicalisation (extreme views)
  - CSE

Responsibilities of Teachers and Support Staff

- Teach pupils about E Safety in line with current legislation.
- Read, understand and promote the school's E Safety policy and guidance.
- Develop and maintain an awareness of current E Safety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed E Safety messages in learning activities where appropriate.
- Report any E Safety related issues that come to your attention to the DSL.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of ICT Technician

- Read, understand, contribute to and help promote the school's E Safety policy and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy.
- Support the school in providing a safe technical infrastructure to support teaching and learning.
- Be responsible for the permissions/security of the school ICT network.
- Report any E Safety related issues that come to your attention to the DSL.
- Develop and maintain an awareness of current E Safety issues, legislation and guidance relevant to your work.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils

- Help and support the school in creating E Safety policies and practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for your own and each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone to whom this is happening.
- Discuss E Safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support your school in promoting E Safety.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.

- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss E Safety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in your own use of technology.
- Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's E Safety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
- Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the school in promoting and ensuring safe and responsible use of technology, including encouraging parents to become engaged in E Safety activities.
- Ensure appropriate funding and resources are available for the school to implement their E Safety strategy.

Teaching and Learning

We believe that the key to developing safe and responsible behaviour online, not only for pupils but everyone, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

- We will provide a series of specific E Safety-related lessons as part of the Computing / PSHRE curriculum.
- We will promote E Safety through assemblies, staff training and whole school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant E Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- We will remind pupils about their responsibilities when using the Internet, and refer them to the Acceptable Use Policy that their parents/carers have signed.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- Include useful links and advice on E Safety regularly in newsletters and on our school website.

Managing ICT Systems and Access

We have a responsibility as a school for ensuring that access to the ICT network is as safe and secure as possible. Servers (both physical and virtual), switches, workstations and other key hardware and infrastructure will be located securely, with only appropriate staff permitted access.

- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed and updated regularly. All users will adhere to an Acceptable Use Policy appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using the school ICT network and that such activity will be monitored and checked.
- All pupils will access the school network and Internet using an individual log-on, which has restricted, monitored access to the network.
- **Pupil internet access should ALWAYS be supervised by a member of staff.**
- Members of staff will access the Internet using a common log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on.
- The administrator password for the ICT Network should be kept secure and available to at least two members of staff, e.g. Head of ICT and/or teacher or a member of technical support.
- No student should be left unaccompanied with ICT equipment.
- The school wireless network will be password controlled and the password will be known only by staff so that unauthorised users nearby cannot inadvertently or deliberately connect.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit ICT use to establish if the E Safety policy is adequate and that the implementation of the E Safety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet access

- The school uses a filtered Internet service. The filtering is put in place by our identified ICT support. We currently use the 'Securly' web filter and safeguarding system, which alerts the DSL to all potential violations or risks immediately via e-mail, which can then be interrogated. This includes users trying to access blocked sites, users typing in trigger words, eg radicalisation, sexual exploitation etc.
- If users discover a website with inappropriate content, they should still report to a member of the SLT or DSL team immediately, who will inform the ICT technician and relevant action will be taken ASAP to block the specific content.
- The DSL and ICT support service will meet half termly with the safeguarding governor to review the filtering, and other security systems to ensure they meet the need of all users.

Use of digital photographs and video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the storing, sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission or parent/ carer consent.
- Written permission from parents or carers will be obtained on an annual basis before photographs of students/pupils or their name are displayed on school displays, in newsletters and in their child's own and other children's learning journeys.
- Written permission from parents or carers will be obtained on an annual basis before photographs of students/pupils or their name are published in leaflets, posters, documents, training materials or used by the press.
- Written permission from parents or carers will be obtained on an annual basis before photographs of students/pupils are published on the school website or social media. Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Photographs of staff and pupils are retained for a maximum of 3 years after leaving, if we have consent to retain the images for this period.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. More detailed guidance on the collection, handling and storage of personal data can be found in the school's General Data Protection Policy.

Learning technologies in school

- **Personal mobile phones brought into school**
  Pupils are **not** allowed to have phones in school. If pupils need to bring a phone in, they sign it in at the start of the day and collect at the end of the school day. Staff are allowed to bring in personal mobile phones but these are not allowed to be used in public areas of the school including classrooms and corridors; they can only be used in the staffroom.

- **Taking photographs or videos on personal equipment**
  Not allowed - staff or pupils

- **Taking photographs or videos on school equipment**
  Pupils allowed, staff allowed of pupils for whom consent has been given

- **Use of hand-held devices such as MP3 players, i-pads, i-pods, tablets or personal gaming consoles**
  Sixth form students allowed MP3 players during supervised breaks.
  Identified students for whom device provides communication and/ or agreed information sharing via wiki-me permitted supervised by staff at all times.

- **Use of personal email accounts in school**
  Pupils and staff not allowed

- **Use of web based email address for personal correspondence**
  Pupils not allowed, staff allowed in staff room

- **Use of online chat rooms**
  Not allowed - staff or pupils

- **Use of instant messaging services**
  Pupils not allowed, staff allowed in staff room

- **Use of blogs, wikis, podcasts**
  Pupils and staff allowed

- **Use of social networking sites**
  Not allowed - staff or pupils

- **Use of video conferencing or other online video meetings**
  Staff allowed at all times, pupils allowed with direct supervision

This policy was recommended for approval by the Children, Families and Community Committee and subsequently approved by the Full Governing Body.
To be reviewed annually.

Signed _____Date _____