Westfield Primary Academy
Online Safety Policy

1.Scope of the Policy

This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, visitors and community users, who have access to and are users of ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school

2.Roles and Responsibilities

The following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Governors :

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Members of the Governing Body have taken on the roles of Safeguarding Governor and Online Safety Governor.

The role of these governors will include:

- Regular meetings with the Online Safety Lead;
- Regular monitoring of online safety incident logs;
- Reporting to Governors' meetings.

Headteacher and Senior Leaders :

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see Procedure for Acceptable Use of ICT Policy).
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.
- The Headteacher will ensure that there is support for those colleagues through update meetings.

Online Safety Lead

The school has an Online Safety Lead who:

- Reports to the Health and Safety Committee and/or Full Governing Body.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents.

• Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
• Provides training and advice for staff.
• Liaises with the Local Authority and/or Trust as required, including technical support staff.
• Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
• Meets termly with the Online Safety Governor to discuss current issues and review incident logs.
• Attends relevant meetings.
• Reports regularly to the Senior Leadership Team.

Teaching and Support Staff
Teachers and support staff are responsible for ensuring that:
• They have an up to date awareness of online safety matters and of the current school Online Safety Policy.
• They have read, understood and signed the Staff Acceptable Use Agreement.
• They report any suspected misuse or problem to the Headteacher/Online Safety Lead (or to the Chair of Governors if the suspected misuse is against the Headteacher).
• All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems.
• Online safety issues are embedded in all aspects of the curriculum and other activities.
• Pupils understand and follow the online safety and acceptable use policies.
• They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities.
• In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead
The DSL and alternates should be trained in online safety issues and be aware of potential for serious safeguarding issues to arise from:
• Sharing of personal data.
• Access to illegal/inappropriate materials.
• Inappropriate online contact with adults or strangers.
• Potential or actual incidents of grooming.
• Cyberbullying.
• Radicalisation or extremism.

Where there are safeguarding concerns, an online safety incident will be recorded using the appropriate concern form.

Computing and PSHE Leaders
The Computing and PSHE Leaders will assist the Online Safety Lead with:
• The production, review and monitoring of the school Online Safety Policy.
• Mapping and reviewing the online safety curricular provision, ensuring relevance, breadth and progression.
• Consulting stakeholders, including other staff and pupils, about online safety provision.
• Monitoring the implementation of agreed curricular improvement actions.

Pupils
The pupils:
• Are responsible for using the school digital technology systems in accordance with Acceptable Use of ICT Policy.

• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
• Will be expected to understand and use the policies on the use of mobile devices and digital cameras.
• Should know and understand policies on the taking and use of images, and on cyberbullying.
• Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers
Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and information about online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:
• Digital and video images taken at school events.

.

3.How Will We Use The Internet Safely To Enhance Learning?

Pupils:
The education of pupils in online safety is an essential part of our school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.
Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression.
This will include:
• A planned online safety curriculum provided as part of Computing lessons, which should be regularly revisited in Computing and PSHE lessons.
• Key online safety messages that will be reinforced as part of assemblies.
• Lessons that teach pupils to be critically aware of the content they access online and to validate the accuracy of information.
• Development of pupils' understanding of the need to adopt safe and responsible use both within and outside school and the importance of the school's Acceptable Use of ICT Policy.
• Staff acting as good role models in their use of digital technologies, the internet and mobile devices.
• Checking of sites suitable for pupils' use and ensuring processes are in place for dealing with any unsuitable material that is found in internet searches.

Parents/Carers
Parents have a crucial role in educating and protecting pupils when using digital technologies. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:
• Letters, newsletters, school website, app etc.
• Information evenings.
• High profile events/campaigns, e.g. Safer Internet Day.

Staff/Volunteers
It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A planned programme of formal online safety training will be made available to staff and, in addition; will be included in safeguarding training and updates.

• All new staff will be required to sign the Acceptable Use Agreement as part of their induction.

• The Online Safety Lead will receive regular updates through attendance at external training events.

• This Online Safety Policy and its updates will be presented to and discussed by staff in staff and team meetings.

• The Online Safety Lead will provide advice and training to individuals as required. The Local Authority has produced presentations to assist with this training.

4.Maintenance of Information Systems

Technical staff

The school employs an IT technician who is responsible for ensuring that:

• The school's technical infrastructure is secure and is not open to misuse or malicious attack.

• The school meets required online safety technical requirements and any Trust Online Safety Policy that may apply.

• Users may only access the networks and devices through a properly enforced password protection policy.

• Suitable filtering is applied and updated on a regular basis.

• They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

• Any misuse of the network is reported to the Headteacher and Online Safety Lead for investigation and action (or to the Chair of Governors if the suspected misuse is against the Headteacher).

Emails

Users may only use approved e-mail accounts.

Emails sent from a school email address to external organisations should be written carefully, in the same way as a letter written on school headed paper would. Email subscriptions using the school email address to websites and other electronic services should be for school and curriculum use only.

Authorisation is required when publishing, sharing or distributing any personal information about pupils and staff (such as, photographs, home address, e-mail address, telephone no. etc)

5.Publication of Pupils Images and Work

Pupils full names will not be used anywhere on the website or open blog.

Photographs will only be published on the school website, app, Twitter, Facebook page and Class Dojo (and only with the permission of the parent/carer).

6. Management of Social Networking (including You Tube)

The Academy will control access to social networking sites through existing filtering systems.

•Pupils and staff are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school/education setting or other establishment name, groups or clubs attended, IM and email address or full names of friends).

•Pupils are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school/education setting or other establishment uniform).

• Pupils are advised on social networking security and recommendations made for privacy settings to be activated to the highest protection setting. The importance of passwords and blocking of unwanted communications is also highlighted.

• The Academy is aware that social networking can be a vehicle for cyber bullying. Pupils are encouraged to report any incidents of bullying to a member of staff or trusted adult, allowing for the procedures, as set out in the anti-bullying policy, to be followed.

•The school Facebook page (and other social media pages which may consequently be set up) will be maintained by the Head Teacher and any other person authorised by the Head Teacher.

•Any material that the school believes is illegal must be reported to appropriate agencies eg. Child Exploitation and Online Protection Centre (CEOP).

•If staff or pupils discover unsuitable sites this must be reported to the Computing Lead and DSL who will then take relevant action.

7. Integration of Online Safety Policy

•All children will be made aware of Online Safety rules and these will be posted in areas with internet access. Users will be informed that network and internet use will be monitored.
•All staff, pupils and parents will have to adhere to the schools Online Safety policy and agreement, along with the acceptable use policy.
•All staff and governors will be aware of the Online Safety policy and its application and importance explained.
•Staff training will be provided on Online Safety at appropriate regular intervals.

8.Monitoring and Review

•There will be an annual review of this policy by the Designated Safeguarding Lead and Computing Lead. The updated policy will then be reviewed by the SLT, governing body and all members of staff.

Date Approved	
Signed	)
Minuted	(Date)
Date of Next Review	