Westways Primary School

Online Safety Policy

January 2024

Version 7.0

(This policy will be reviewed annually)

Policy Introduction

This document is an introduction to our approach to Online Safety. We recognise the roles of digital technologies in teaching and learning at Westways Primary School and the potential risks that these can involve.

Scope of the Policy

As well as forming part of the whole school Safeguarding Policy, of which this is an key integral part, this policy applies to all members of the school community (including staff, Governors, pupils, volunteers, parents / carers, work placement students, visitors, community users) who have access to and are users of school computer systems, both in and out of school.

- **The Education and Inspections Act 2006** empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

- **The Education Act 2011** gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others.
  https://www.gov.uk/government/publications/searching-screening-and-confiscation

- The school will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform parents/ carers of incidents of inappropriate Online Safety behaviour that takes place out of school. This includes acting within the boundaries identified in the Department for Education guidance for Searching, Screening and Confiscation.

- **Keeping Children Safe in Education 2023 update** – this is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Education (Non-Maintained Special Schools) (England) Regulations 2011. Schools and colleges must have regard to it when carrying out their duties to safeguard and promote the welfare of children. The document contains information on what schools and colleges **should** do and sets out the legal duties with which schools and colleges **must** comply. It should be read alongside statutory guidance **Working Together to Safeguard Children 2018**

- **Counter-Terrorism and Border Security Act 2019** **(Updated from the 2015 original.)** From 1 July 2015 all schools, registered early years childcare providers and registered later years childcare providers are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”.
  The statutory guidance on the Prevent duty summarises the requirements on schools and childcare providers in terms of four general themes: risk assessment, working in partnership, staff training and IT policies. All staff have undertaken Prevent training.
  https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

Development / Monitoring / Review of this Policy

This policy was developed by a working group including:

- Executive Headteacher/Head of School (Referred to collectively as 'Headteacher' in this document)
- Online Safety Lead
- Teachers
- Governors

It is updated annually by the Online Safety Lead in conjunction with the Safeguarding Lead and Executive Headteacher/Head of School (for ease referred to as 'Headteacher' throughout this document).

Schedule for Development / Monitoring / Review

[Because of the regular updates of the policy there may be many versions created. Each version should be stored for audit purposes.]

Title	**Westways Primary School Online Safety Policy**
Version	7.0
Date	*24/01/2024*
Author	*Online Safety Lead*
Approved by the Governing Body on:	
Monitoring will take place at regular intervals:	*Annually*
The Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	*January 2025*

The school will monitor the impact of the policy using:

- Logs of reported incidents (CPOMS)
- Internal monitoring data for network activity
- Surveys / questionnaires of:
    - students / pupils
    - parents / carers
    - staff

Communication of the Policy

Westways Primary School will communicate with all stakeholders by:

- The senior leadership team will be responsible for ensuring the school community are aware of the existence and contents of the school Online Safety Policy and the use of any new technology as and when appropriate via newsletters and website
- The Online Safety Policy will be distributed and shared with all members of staff & Governors formally.
- An Online Safety training programme has been established across the school (Online Safety & Prevent training) and includes a regular review of the Online Safety Policy.
- Online Safety training will be part of the induction of new staff & new starters to school
- The school approach to Online Safety and its policy is being reinforced through the curriculum.
- The key messages contained within the Online Safety Policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed Online Safety messages across the curriculum whenever the internet or related technologies are used
- The Online Safety Policy will be introduced to the pupils via KS2 School Council and through an assembly/class teachers in KS1 & EYFS.
- Safeguarding posters will be prominently displayed around the setting.

Roles and Responsibilities

We believe that Online Safety is the responsibility of the whole school community and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities technology offers in learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of Governors

Governors are responsible for the approval of the Online Safety Policy and for approving subsequent updates as well as reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of Online Safety Governor.

Responsibilities of the Headteacher

The Headteacher has overall responsibility for safeguarding all 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 senior leadership team are 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 when necessary.
- The Headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal Online Safety role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The Headteacher and senior leadership team will ensure that everyone is aware of procedures to be followed in the event of a serious Online Safety incident.
- The Headteacher and senior leadership team receive update reports of any incidents from the Online Safety/Safeguarding team.

Responsibilities of the Online Safety Lead

We have named leads for safeguarding and Online Safety whose role is:

- To ensure that the school Online Safety Policy is current and relevant.
- To ensure that the school Online Safety Policy is systematically reviewed at agreed time intervals.

- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.
- To promote an awareness and commitment to Online Safety throughout the school.
- To be the first point of contact in school on all Online Safety matters.
- To take day-to-day responsibility for Online Safety within school and to have a leading role in establishing and reviewing the school Online Safety policies and procedures.
- To communicate regularly with school technical staff.
- To communicate regularly with the designated Online Safety Governor.
- To communicate regularly with the senior leadership team.
- To create and maintain Online Safety policies and procedures.
- To develop an understanding of current Online Safety issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in Online Safety issues.
- To ensure that Online Safety education is embedded across the curriculum.
- To ensure that Online Safety is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on Online Safety issues to the senior leadership team using CPOMS.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident.

Responsibilities of the Teaching and Support Staff

- To understand, contribute to and promote the school's Online Safety policies and guidance.
- To understand and adhere to the school Staff Acceptable Use Policy (see Appendix 2).
- To report any suspected misuse or problem to the Online Safety Lead or senior leadership team as appropriate.
- To develop and maintain an awareness of current Online Safety issues and guidance including online exploitation, radicalisation and extremism, bullying, sexting etc.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media etc.
- To embed Online Safety messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To be aware of Online Safety issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms within the school.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by using only approved and encrypted data storage and by transferring data through secure communication systems.

Responsibilities of the Technical Staff

The school will ensure that the managed service provider carries out all the Online Safety measures, as outlined below.

- To understand the school's Online Safety policies and guidance.
- To understand and adhere to the school Staff Acceptable Use Policy (see Appendix 2).

- To report any Online Safety related issues that come to your attention to the Online Safety Lead.
- To develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to their work such as the Prevent Duty.
- To maintain a professional level of conduct in their personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the senior management team, local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Protecting the professional identity of all staff, Governors, work placement students and volunteers

Communication between adults and children, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, emails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff, Governors and volunteers should:

- Only make contact with children for professional reasons and in accordance with the policies and professional guidance of the school.
- Not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- Not request, or respond to, any personal information from the child other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Not send or accept a friend request from the child or parent/carers on social networks.
- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- Ensure that all communications are transparent and open to scrutiny.
- Be careful in their communications with children, parent/carers so as to avoid any possible misinterpretation.
- Ensure that if they have a personal social networking profile, details are not shared with children in their care or parents/carers (making every effort to keep personal and professional online lives separate).
- Not post information online that could bring the school into disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Designated Safeguarding Lead

- To understand the issues surrounding the sharing of personal or sensitive information and to ensure that personal data is protected in accordance with the Data Protection Act 2018.
- To understand the risks and dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving the grooming of children and young people in relation to sexual exploitation, radicalisation and extremism.
- To be aware of and understand online bullying and the use of social media and online gaming for this purpose.

Responsibilities of the Pupils

- Understand and adhere to the school pupil Acceptable Use Policy.
- To help and support the school in the creation of Online Safety policies and practices and to adhere to those the school creates.
- To know and understand school policies on the use of digital technologies including mobile phones, digital cameras and any other personal devices.
- To know and understand school policies on the use of mobile phones in school.
- To know and understand school policies regarding cyberbullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the potential risks such as online exploitation, radicalisation, sexting and online bullying.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss Online Safety issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support the school in promoting Online Safety.
- To read, understand and promote the school's Online Safety Policy and the pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss Online Safety concerns with their children, be aware of what content, websites and Apps they are using, apply appropriate parental controls and ensure they behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology and social media including matters relating to the school and with particular reference to ensuring the good reputation of the school is upheld.
- To consult with the school if they have any concerns about their children's use of the internet and digital technology.

- School admission procedures explain clearly the use of photographic and video images within or outside of school.

On admission to school, parents/carers sign to agree to:

- Support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community.
- Support the school's Online Safety Policy.
- Ensure images taken of pupils at school events will be for personal use only and not uploaded or shared via the internet.
- Take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.
- Read through and sign acceptable use agreements on behalf of their children on admission to school
- Give consent for the use of any images of their children in a variety of different circumstances (i.e. 'internal'; 'internal and external')

Education

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a safe and responsible approach. The education of pupils in Online Safety is therefore an essential part of Westways Online Safety provision. Children need the help and support to recognise and mitigate risks and build their resilience online.

Online Safety is part of a broad and balanced curriculum and staff will reinforce Online Safety messages. The Online Safety curriculum is broad, relevant and provides progression, with opportunities for creative activities. This will be provided in the following ways:

- A planned Online Safety curriculum is provided as part of Computing & PHSE using the Sheffield RHE scheme of work.
- Key Online Safety messages are reinforced as part of a planned programme of assemblies including promoting Safer Internet Day each year.
- Pupils are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- We will discuss, remind or raise relevant Online 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.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- It is accepted that from time to time, for good educational reasons, staff may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study.

- In lessons where internet use is pre-planned, pupils are 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
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the children visit.
- All use will be monitored and they will be reminded of what to do if they come across unsuitable content.
- Pupils are taught about the impact of online bullying and know how to seek help if they are affected by any form of bullying.
- Pupils are made aware of where to report, seek advice or help if they experience problems when using the internet and related technologies; e.g. parent/ carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

All Staff (including Governors)

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:

- All staff receive regular information and Online Safety training through a planned programme of regular updates. These updates are usually led by a member of the Sheffield e-learning team.
- All new staff receive Online Safety information and guidance as part of the induction process, ensuring that they fully understand the Online Safety and Acceptable Use Policies.
- All staff are made aware of individual responsibilities relating to the Online Safety of children and know what to do in the event of misuse of technology by any member of the school / college community.
- An audit of the Online Safety training needs of all staff will be carried out at least annually..
- The Online Safety Lead and CPLT will provide advice, guidance and training as required.

Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in a safe and responsible way and in promoting the positive use of the internet and social media. Many have only a limited understanding of Online Safety risks and issues, yet it is essential they are involved in the Online Safety education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may under-estimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Westways will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, dedicated website page
- Bi-annual Parents / Carers 'training event' run by Sheffield Online Safety lead.
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any group involved in technology / Online Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Safeguarding Children Board / Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Sheffield City Council eLearning Service has been commissioned by Sheffield Safeguarding Children Board to deliver Online Safety training to schools and settings in the city.

As part of the Parent / Carer training event; a member of the Sheffield e-learning team conducts an Online Safety 'survey' with small groups of pupils from Y2 to Y6. The findings and outcomes from this are fed back to school where staff in the respective year groups are given copies of the information. This information is also used during the Parent / Carer training event to disclose to parents what the children at Westways admit to doing online. This will become an annual event as of 2022/2023..

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's Online Safety knowledge and experience. This may be offered through the following:

- Online Safety messages are targeted towards grandparents and other relatives as well as parents.
- The school website provides Online Safety information for the wider community.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to teaching and learning, allowing staff and pupils instant use of images that they have uploaded themselves or downloaded from the internet. However, everyone needs to be aware of the potential 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 their legal responsibilities and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff will inform and educate pupils about the risks and current law associated with the taking, sharing, use, publication and distribution of images. In particular they should recognise the risks attached to publishing inappropriate images on the internet or distributing through mobile technology.

- Staff are allowed to take digital / video images to support educational aims or promote celebrations and achievements, but must follow school policies concerning the sharing, distribution and publication of those images.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Staff will be aware of those pupils where publication of their image may put them at risk.

- Pupils' full names are not used in association with photographs.

- Written permission from parent or carers is obtained before photographs of pupils are published on the school website or in the local media. Each class teacher has a list of pupils whose parents have provided such permission.

- Pupil's work can only be published with the permission of the pupil and parent or carers.

- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Managing ICT systems and access: Technical infrastructure, equipment, filtering and monitoring

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible and meets recommended technical requirements.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.
- The infrastructure and appropriate hardware are protected by active, up to date virus software (SMOOTHWALL)
- There will be regular reviews and audits of the safety and security of technical systems.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- The “master / administrator” passwords for the school computer system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- All users will have clearly defined access rights to school technical systems and devices.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- In Key Stage 2, pupils will have an individual log-in with an appropriate password which will be kept secure. They will ensure they log out after each session.
- Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID and password. They will abide by the staff AUP at all times.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by Smoothwall Firewall.
- The school’s internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed, sent or received through the school’s internet provision.
- The school ensures that the filtering system blocks extremist content and protects against radicalisation in compliance with the Counter-Terrorism and Border Security Act 2019.
- The school have a clearly defined procedure for reporting breaches of filtering. All staff (and pupils) will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online Safety Lead. All incidents will be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety Lead.
- The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the Internet Watch Foundation IWF.
- The school will regularly review the effectiveness of SMOOTHWALL.

- The school filtering system blocks all sites on the Internet Watch Foundation list and Government Prevent block list and this will be kept updated.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Passwords

Passwords are an important aspect of computer security. They are the front line of authentication for the protection of user accounts and their associated access to ICT equipment and resources. A poorly-chosen password may result in the compromise of a pupil's work, sensitive information regarding pupils or staff being lost or stolen or a school/college network being infected or attacked. The school has a responsibility to ensure that all elements of the school infrastructure and network equipment are as safe and secure as possible. All staff and pupil access to school-owned equipment and information assets should be controlled through the use of appropriate username and password policies.

It is important that all pupils and staff have an awareness of how to construct a complex and secure password as well as understanding the security implications of not protecting the password once selected.

Key steps:

- The School Manager and IT Technician assess the risk of using different technologies in school.
- Once this process has been completed, appropriate controls should be highlighted and recommendations made regarding what access should be protected through the use of usernames and passwords.
- Once this has been established, suitable technical controls and authentication mechanisms should then be implemented.

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- EYFS pupils have a generic login to all school ICT equipment.
- Pupils in Key Stage 1 have a class based, user account log-in and password for access to ICT equipment and information systems available within school.
- Pupils in Key Stage 2 will have an individual, user account log-in and password for access to ICT equipment and information systems available within school.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems.
- All information systems require end users to change their password at first log on.
- Staff users are prompted to change their passwords every September or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.

All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords.

- Do not write down system passwords.
- Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
- Always use your own personal passwords to access computer based services, never share these with other users.
- Make sure you enter your personal passwords each time you login. Do not include passwords in any automated login procedures.
- Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Users should create different passwords for different accounts and applications.
- Users should be encouraged to use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

Management of assets

- Details of all school-owned hardware will be recorded in an inventory held by the School Business Manager.
- Details of all school-owned software will be recorded in a software inventory held by the School Business Manager.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment (Amendment) Regulations 2018

Data Protection

Personal Data

The school may have access to a wide range of personal information and data, held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about children / young people, members of staff / volunteers / students and parents / carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by mothers and fathers / carers or by other agencies working with families

The Data Protection Act 2018 requires every organisation processing personal data to notify with the Information Commissioner's Office, unless they are exempt.

All schools must understand the implications of not securing the information assets they hold and should look to appoint a Senior Information Risk Officer (SIRO) This role may well be combined with the schools Data Protection Officer and, where appropriate, Information Asset Owners (IAO).

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

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

Westways will:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data or their computer is locked when left unattended.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted
    - the device must be password protected
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email or post) should be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations. They can only be taken off site with written permission from the Headteacher or School Business Manager.

Secure Transfer Process

If sensitive information or personal data is being transmitted electronically it must be transferred by a secure method so it is protected from unauthorised access (e.g. anycomms)

Email

Staff do not use public email accounts for sending and receiving sensitive or personal data.

DO NOT include personal or sensitive information within the email itself, as the information sent should be by a secure method. This can be done by creating a document (e.g. Word document) and then password protecting the document and sending it as an attachment with the e-mail. The password should be sent in a separate e-mail.

Encryption makes a file non readable to anyone who does not have the password to open it, therefore, it reduces the risk of unauthorised people having access to the information and protects staff from breaching the law.

Communication Technologies

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✔						✔*	
Use of mobile phones in lessons				✔				
Use of mobile phones in social time	✔							✔
Taking photos on mobile phones/cameras or other devices				✔				✔
Use of other mobile/hand held devices	✔							✔
Use of personal email addresses in school, or on school network		✔						✔
Use of school email for personal emails				✔				✔
Use of messaging Apps				✔				✔
Use of social media				✔				✔
Use of blogs	✔					✔		

* Pupils bringing mobile phones to school must hand them into the school office at the beginning of the day and collect them, at home time.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored

- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any agreed channel of digital communication between staff and pupils or parents / carers must be professional in tone and content.

User Actions:		Acceptable	Acceptable at certain times	Acceptable for certain users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✔
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✔
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✔
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 Radicalisation or extremism in relation to the Counter Terrorism and Security Act 2015					✔
	pornography				✔	
	promotion of any kind of discrimination				✔	
	threatening behaviour, including promotion of physical violence or mental harm				✔	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✔	
Using school systems to run a private business					✔	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					✔	
Infringing copyright					✔	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					✔	
Creating or propagating computer viruses or other harmful files					✔	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					✔	
On-line gaming (educational)			✔			

On-line gaming (non educational)				✔	
On-line gambling				✔	
On-line shopping / commerce			✔		
File sharing	✔				
Use of social media				✔	
Use of video broadcasting eg Youtube			✔		

Unsuitable / inappropriate activities

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

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material, radicalisation and extremism
- other criminal conduct, activity or materials

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils:

Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Headteacher or other member of SLT	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			✔	✔		✔		✔	
Unauthorised use of non-educational sites during lessons			✔			✔		✔	
Unauthorised use of mobile phone / digital camera / other handheld device		✔				✔			
Unauthorised use of social networking / instant messaging / personal email		✔				✔			
Unauthorised downloading or uploading of files		✔				✔			
Allowing others to access school network by sharing username and passwords		✔				✔			
Attempting to access or accessing the school network, using another student's / pupil's account		✔				✔			
Attempting to access or accessing the school network, using the account of a member of staff			✔			✔		✔	
Corrupting or destroying the data of other users			✔			✔		✔	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			✔	✔		✔			
Continued infringements of the above, following previous warnings or sanctions			✔			✔			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✔			✔			
Using proxy sites or other means to subvert the school's filtering system			✔			✔		✔	
Accidentally accessing offensive or pornographic material and failing to report the incident	✔								
Deliberately accessing or trying to access offensive or pornographic material			✔			✔			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✔							

Staff:

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			✔	✔			✔	✔
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✔	✔			✔		
Unauthorised downloading or uploading of files		✔	✔			✔		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✔	✔			✔		
Careless use of personal data eg holding or transferring data in an insecure manner		✔						
Deliberate actions to breach data protection or network security rules		✔	✔					✔
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✔	✔					✔
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✔	✔	✔				✔
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		✔						
Actions which could compromise the staff member's professional standing		✔						✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✔				✔		
Using proxy sites or other means to subvert the school's filtering system		✔				✔		
Accidentally accessing offensive or pornographic material and failing to report the incident		✔						
Deliberately accessing or trying to access offensive or pornographic material		✔		✔				✔
Breaching copyright or licensing regulations		✔						
Continued infringements of the above, following previous warnings or sanctions		✔	✔			✔		✔

Dealing with Online Complaints

The nature of the internet, and the two-way communication that it brings, means that many parents will now turn to the online world to air their concerns or grievances. Schools often find that a seemingly minor incident can escalate quite quickly with Facebook pages or groups being formed where parents can discuss issues and gather support. It is advised that there should be a procedure for dealing with online complaints, particularly in relation to derogatory comments made in social networks by parents/carers or other members of the school community.

Managing your school digital footprint is as crucial as managing a personal one. This is equally important for schools that have a social-media presence as well as those with just a website. Staff must understand the importance of not being drawn into discussions or reacting to complaints. It is vital that all staff, governors, pupils and parents are aware that official complaints channels exist and that the internet, particularly social media, is not a recognised option.

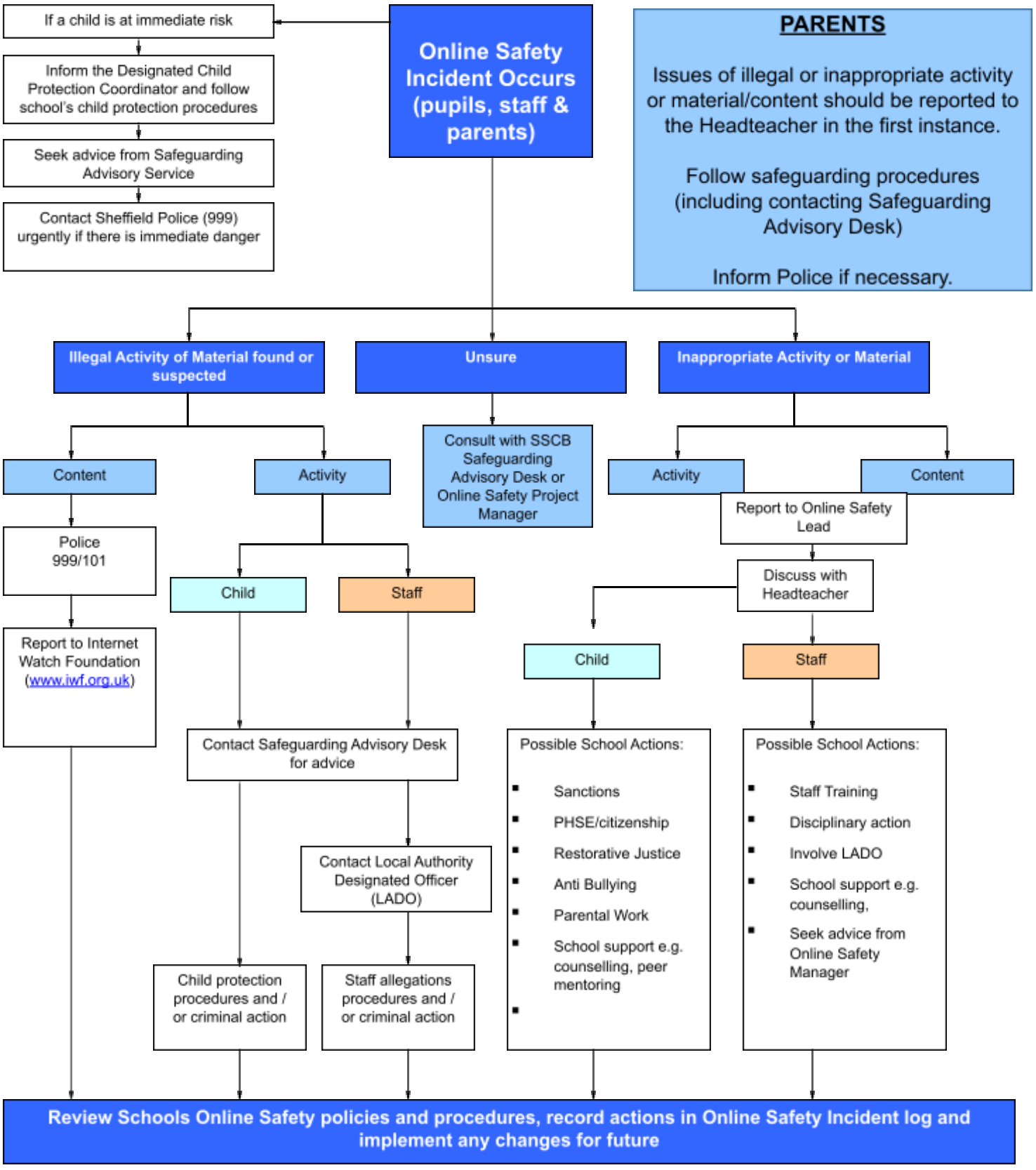
Key Steps:

1) Ensure that all staff and governors are aware of how to report and react to negative online statements
2) Review your Acceptable Use Policies to ensure that they clearly state that staff and governors must not be drawn in to any online discussions.
3) Review and update your complaints procedure to include reference to not utilise online channels for complaints.

- Parents/Carers are reminded through the admissions procedures / website of appropriate complaints channels and procedures.
- The complaint policy/procedure is clearly detailed on the school website and within the Complaints Policy.
- All staff and governors are aware of how to report any negative online comments about the school or members of the school community.
- Staff and Governors must under no circumstances reply or react to any online discussion about the school unless prior permission has been granted by the Headteacher.

Appendix 1

Response to an Incident of Concern



Appendix 2

Staff Acceptable Use Policy

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign to acknowledge they have read and agreed this policy which should be adhered to at all times. All concerns and clarification should be discussed with Martin Fallon (Executive Headteacher) or Charles Hollamby (Head of School).

- I will only use the school's email/internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal details such as mobile phone number and personal email address to pupils.
- I will only use the approved, secure Gmail email address for any school business.
- I will ensure personal data is kept secure and is used appropriately, whether in school or taken off school premises.
- I will not use USB drives, portable hard drives, or personal laptops on the network without having them approved by the school and/or encrypted.
- I will not install any hardware or software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will ensure that I log off after my session has finished.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes and with the consent of the parent/carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.
- I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team. Any images taken on personal cameras/phones will be stored at school and deleted from the device before the end of the school day.
- I understand that all my use of the internet and other related technologies can be monitored by the Headteacher.
- I will support the school's approach to online safety and not deliberately upload or add any images, videos, sounds or text that could upset or offend any member of the school community
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will not accept invitations from children and young people or their families to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.
- As damage to professional reputations can be inadvertently caused by quite innocent postings or images – I will be careful with who has access to my pages through friends and friends of friends. This applies to those connected with my professional duties such as parents and their children.
- I will support and promote the school's online safety and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand that this policy should be read alongside the Westways Code of Conduct.

I have read and understood the information detailed above.

Name: _____ Date: _____

Signed: _____