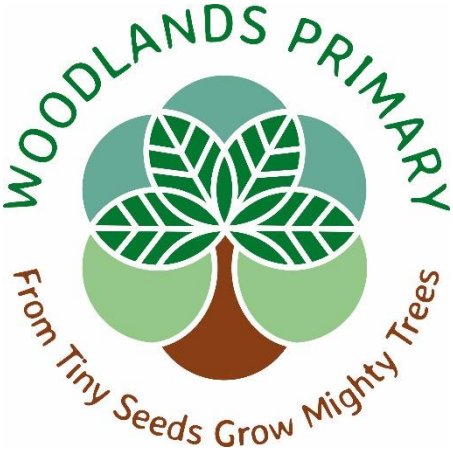


Online Safety Policy

Date: June 2021

Online Safety Lead	**Lisa Lock**
Online Safety Team	**Lisa Lock** **Wendy Scott** **Lauren Johnstone**
DSL	**Wendy Scott**
DSD	**Lauren Johnstone** **Sam Herring** **Katie Hall** **Sarah Bustamante** **Abby-Jo Stacey** **Vikki Taylor**

Date ratified	**22/06/21**
Governors/Committee Meeting	**Governors**
Signature of Chair	**Dawn Bogunvic**
Date for Review	**22/06/22**

Introduction

Online safety is an integral part of safeguarding pupils at Woodlands. This policy aim is to ensure all individuals who have contact with children are aware of how to safeguard them both in school and out of school. This policy will be reviewed annually and will be amended sooner if required by an online safety incident.

Technology enhances our curriculum and supports pupils with the skills they need for an ever changing digital world. This policy supports pupils to stay safe and ensures that risks are identified, assessed and mitigated.

Scope of the Policy

This policy applies to all members of the school community (including staff, Board of Governors, pupils, volunteers, parents/carers, work placement students, visitors) who have access to and are users of school ICT 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 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 Safeguarding 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/college 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 Safeguarding 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 September 2020** 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 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 2020**

- **Counter-Terrorism and Security Act 2015** 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.

https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

Development of this Policy

This policy has been developed by a working group made up of:

- Headteacher: Lauren Johnstone
- Designated Safeguarding Lead: Wendy Scott
- Online Safety Lead: Lisa Lock
- Staff – including Teachers, Support Staff, Technical staff

Consultation with the whole school has taken place through a range of informal meetings.

Schedule for Development

Title	Woodlands Online Safeguarding Policy
Version	1.0
Date	*05/05/21*
Author	*Online Safety Team*
Approved by the Governing Body on*:*	
Monitoring will take place at regular intervals:	*Termly*
The Governing Body will receive a report on the implementation of the policy including anonymous details of any Online Safeguarding incidents at regular intervals:	*Termly*
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 Safeguarding or incidents that have taken place. The next anticipated review date will be:	*May 2022*
Should serious Online Safeguarding incidents take place, the following external persons / agencies should be informed:	*Lisa Lock (Online Safety Lead)* *Wendy Scott (Designated Safeguarding Lead)* *LA Safeguarding Officer* *Police Commissioner's Office*

The school/college will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students
    - parents / carers
    - staff

Communication of the Policy

- The senior leadership team will be responsible for ensuring members of the school community are aware of the existence and contents of the school online safeguarding policy and the use of any new technology as and when appropriate.
- The online safeguarding policy will be provided to and discussed with all members of staff.
- All amendments will be published and appropriately communicated to all members of the school community.
- The pupil friendly version of the policy will be discussed by the School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An online safeguarding training programme will be established across the school and will include a regular review of the online safeguarding policy.
- Online safeguarding training will be part of the induction programme.
- The school approach to online safeguarding and its policy will be reinforced through the curriculum.
- The key messages contained within the online safeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed online safeguarding messages across the curriculum whenever the internet or related technologies are used.
- The online safeguarding policy will be used regularly with children in every year group.
- Safeguarding posters will be prominently displayed around the setting.

Roles and Responsibilities

We believe that Online Safeguarding 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.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about Online Safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *Online Safety Governor*

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Lead
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

Responsibilities of Headteacher, DSL and Senior Leaders:

The Designated Safeguarding Lead has overall responsibility for safeguarding all members of the school community, though the day to day responsibility for Online Safeguarding may be delegated to the Online Safety Lead.

- The Headteacher, DSL 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 Safeguarding 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 Safeguarding role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the DSL and Online Safety Lead.
- The Headteacher and senior leadership team will ensure that everyone is aware of procedures to be followed in the event of a serious Online Safeguarding incident.
- The Headteacher and senior leadership team receive update reports of any incidents from the Online Safeguarding/Safeguarding team.

Responsibilities of the Online Safeguarding Team

- To ensure that the school Online Safeguarding policy is current and relevant.
- To ensure that the school Online safeguarding 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 ensure that the school has an online safety curriculum and to ensure that this is not solely delivered in Computing.

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 Online Safeguarding Lead

- To promote an awareness and commitment to Online Safeguarding throughout the school.
- To be the first point of contact in school on all Online Safeguarding matters.
- To take day-to-day responsibility for Online Safeguarding within school and to have a leading role in establishing and reviewing the school Online Safeguarding policies and procedures.
- To lead the school Online Safeguarding group or committee.
- To have contact with and access to other Online Safeguarding committees, e.g. Safeguarding Children Board
- To communicate regularly with school technical staff.
- To communicate regularly with the designated Online Safeguarding governor.
- To communicate regularly with the senior leadership team.
- To create and maintain Online Safeguarding policies and procedures.

- To develop an understanding of current Online Safeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in Online Safeguarding issues.
- To ensure that Online Safeguarding education is embedded across the curriculum.
- To ensure that Online Safeguarding 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 Safeguarding issues to the Online Safeguarding group and the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safeguarding incident.
- To ensure that an Online Safeguarding incident log is kept up to date

Responsibilities of the Teaching and Support Staff

- To understand, contribute to and promote the school's Online Safeguarding policies and guidance.
- To understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the Online Safeguarding coordinator.
- To develop and maintain an awareness of current Online Safeguarding issues and guidance including online exploitation, radicalisation and extremism, and peer-on peer abuse e.g. 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 Safeguarding 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 Safeguarding 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.
- Ensure that sensitive and personal data is kept secure at all times by adhering to the school's password and device protection policy e.g. screen locks.

Responsibilities of Technical Staff

- To understand and adhere to the school staff Acceptable Use Policy.
- To report any Online Safeguarding related issues that come to your attention to the Online Safeguarding coordinator.
- To develop and maintain an awareness of current Online Safeguarding issues, legislation and guidance relevant to their work such as the Prevent Duty.
- To maintain a professional level of conduct in your 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 between children and adults, 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, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

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

- only make contact with children and young people 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 pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy.

- To help and support the school in the creation of Online Safeguarding 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 online bullying.
- 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 exist within school.
- To discuss Online Safeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support the school in promoting Online Safeguarding.
- To read, understand and promote the school's Online Safeguarding 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 Safeguarding 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.
- To consult with the school if they have any concerns about their children's use of the internet and digital technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.

To agree to a home-school agreement containing the following statements

- *We will 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*
- *We will support the school's Online Safeguarding Policy.*
- *Parents may take photographs at school events of their own child/ren: 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.*
- *Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school*

- *Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.*

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 the school's Online Safety provision. Children and young people need the help and support to recognise and mitigate risks and build their resilience online.

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

- A planned Online Safety curriculum will be provided as part of Computing / Wellbeing and other lessons and should be regularly revisited.
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities, including promoting Safer Internet Day each year.
- Pupils will be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Pupils will be 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.
- In lessons where internet use is pre-planned, it is best practice that 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
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of bullying.
- Pupils will be made aware of where to report, seek advice or help if they experience problems when using the internet and related technologies; e.g. parent or 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 will receive regular information and Online Safeguarding training through a planned programme of regular updates.
- All new staff will receive Online Safety information and guidance as part of the induction process, ensuring that they fully understand the Online Safeguarding policy and Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the Online Safeguarding of children and know what to do in the event of misuse of technology by any member of the school community.
- This Online Safeguarding policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- An audit of the Online Safety training needs of all staff will be carried out regularly.
- The Online Safety Lead 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.

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

- Curriculum activities
- Letters, newsletters, website & Class Dojo
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant websites / 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 Online Safety and 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 sessions for staff or parents (this may include attendance at assemblies / lessons).

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. Those images should only be taken on school equipment, the personal equipment, including mobile phones, 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.
- 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 will not be used in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil.
- 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

Possible statements

- 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.
- 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 / college ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg safe)
- 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.

- At Key Stage 2 (and above), pupils will have an individual user account provided with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Policy. 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 appropriate system is in place for users to report any technical incident or security breach.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that staff / pupils are allowed on school devices that may be used out of school.
- An agreed policy regarding the removal of access to network, email, cloud services, and devices for staff and student leavers.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / portable hard drives, 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

Consider the issues in the following statements, and discuss how you will address these within your school. Then adapt or replace the statements to reflect your approach.

- The school uses a filtered internet service. The filtering system is provided by Smoothwall.
- 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 will ensure that the filtering system will block extremist content and protect against radicalisation in compliance with the Prevent Duty, Counter-Terrorism and Security Act 2015
- The school will 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 regularly review the filtering product for its effectiveness.
- Any amendments to the school filtering policy or block-and-allow lists will be checked, risk assessed and recorded by the DSL or their representative 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

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Key Stage 1 pupils will have a generic 'pupil' logon to all school ICT equipment.
- Pupils at Key Stage 2 and above will have a unique, individually-named user account 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.
- Users will be prompted to change their passwords every 6 months 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 agree to 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, e.g.
- 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 logon. Do not include passwords in any automated logon 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.
- Passwords should comply with current accepted complexity recommendations.

Data Protection

Please see Data Protection Policy.

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	X						X	
Use of mobile phones in lessons				X				
Use of mobile phones in social time	X							X
Taking photos on mobile phones/cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices				X				X
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of messaging Apps				X				X
Use of social media				X				X
Use of blogs	X						X	

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 intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Dealing with Online Complaints

- Parents/Carers are reminded through the Home-School Agreement 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.

Contacts

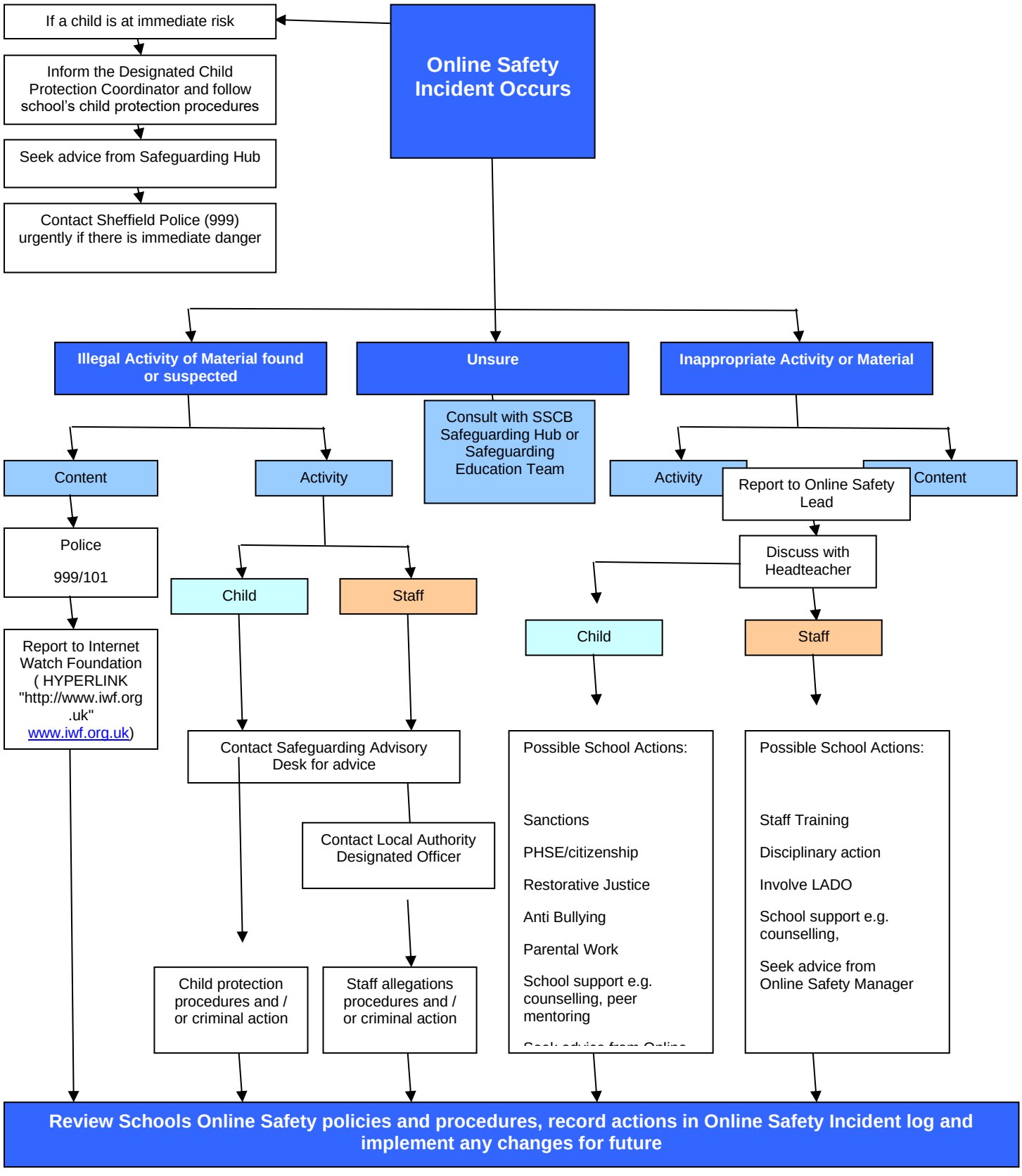
Sheffield Safeguarding Hub 0114 2734855

Sheffield Police 101

Local Authority Designated Officer (LADO) 2734628

WOODLANDS PRIMARY
From Tiny Seeds Grow Mighty Trees

Response to an Incident of Concern



Contact Details