

*Woodlands Academy of
Learning*

E-Safety Policy

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group / committee made up of:

- ✓ Mrs Newton Head teacher
- ✓ Miss S Harvey E-Safety Coordinator
- ✓ Mrs J Graham Deputy Safeguarding lead
- ✓ Mrs L Garcha – Assistant Head/ Maths Leader
- ✓ Mr Ian Whitehouse –Governor
- ✓ Mr Erik West – Parent Governor/ Link curriculum governor
- ✓ Nicola Rudge – Local Authority Esafety advisor

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

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the <i>Governing Body</i>	Yes
The implementation of this e-safety policy will be monitored by the:	<i>Miss S Harvey – Esafety Lead, Erik West – Link curriculum governor and Ian Whitehouse – safeguarding governor</i>
Monitoring will take place at regular intervals:	<i>Half termly</i>
The <i>Governing Body</i> will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	<i>January 2019</i>
The E-Safety 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 e-safety or incidents that have taken place. The next anticipated review date will be:	<i>January 2019</i>
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	<i>Mrs T Newton – Head teacher Mrs J Graham – Deputy Safeguarding Lead</i>

The school will monitor the impact of the policy using:

- ✓ Logs of reported incidents including CPOMs
- ✓ Monitoring logs of internet activity (including sites visited)
- ✓ Internal monitoring data for network activity (Policy Central)
- ✓ Surveys / questionnaires of
 - students / pupils
 - parents / carers
 - staff

Aim of the Policy

It is the responsibility of everyone at woodlands to promote and teach online safety to all children so that every child knows age appropriate strategies to keep them safe online.

All staff/ adults to:

- Highlight the positives of using the internet and the opportunities it presents.
- Think carefully before safeguarding (see flowchart)
- Recognise that young people use the internet in different ways.
- Create a culture of open dialogue
- Be interested, ask questions and listen to young people's views.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for Behaviour policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the academy.

Governors

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

- ✓ regular meetings with the E-Safety Co-ordinator
- ✓ regular monitoring of e-safety incident logs
- ✓ regular monitoring of filtering / change control logs
- ✓ reporting to relevant Governors / Board / committee / meeting

Head teacher

- ✓ The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator
- ✓ The Head teacher as Designated Safeguarding Lead and Deputy Safeguarding Leads are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See Safeguarding and Child Protection Policy)
- ✓ The Head teacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- ✓ The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. As a model of good practice Mrs T Newton, Mrs C Macpherson, Miss S Harvey and Mrs A Fieldhouse receive the reports from Policy Central.
- ✓ The Head teacher will ensure that the use of the network / internet / email is regularly monitored in order that any misuse / attempted misuse is reported to them.

E-Safety Coordinator

- ✓ Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ✓ Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place (following the Safeguarding procedures).
- ✓ Provides training and advice for staff
- ✓ Liaises with the Local Authority / relevant body
- ✓ Liaises with school technical staff
- ✓ Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- ✓ Meets regularly with E-Safety Governor to discuss current issues, review incident logs.
- ✓ Attends relevant meeting of Governors
- ✓ Will ensure that the use of the network / internet / email is regularly monitored in order that any misuse / attempted misuse is reported to the Head teacher.

Network Manager / Technical staff:

The *Technical Staff* are responsible for ensuring:

- ✓ That the academy's technical infrastructure is secure and is not open to misuse or malicious attack.
- ✓ That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- ✓ The filtering programme is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- ✓ That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- ✓ That monitoring software / systems are implemented and updated as agreed in academy policies.

Teaching and Support Staff

The teaching and support staff are responsible for ensuring that:

- ✓ They have an up to date awareness of e-safety matters and of the current academy e-safety policy and practices
- ✓ They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- ✓ They report any suspected misuse or problem to the Head teacher / Senior Leaders/ E-Safety Coordinator / Officer for investigation / action / sanction
- ✓ All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- ✓ E-safety issues are embedded in all aspects of the curriculum and other activities
- ✓ Pupils understand and follow the e-safety and acceptable use policies
- ✓ Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- ✓ They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- ✓ In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

The designated safeguarding lead should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- ✓ sharing of personal data
- ✓ access to illegal / inappropriate materials
- ✓ inappropriate on-line contact with adults / strangers
- ✓ potential or actual incidents of grooming
- ✓ cyber-bullying

Pupils:

- ✓ Are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Policy
 - ✓ Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
 - ✓ Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
 - ✓ Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
 - ✓ Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the academy's E-Safety Policy covers their actions out of school, if related to their membership of the school
- ✓ Digital leaders from years 6, 5 and 4 were trained in January 2017.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- ✓ Digital and video images taken at school events
- ✓ Access to parents' sections of the website / pupil records
- ✓ (See appendix for Policy for parents and film.)

If pupil devices are brought into school they are to be given to the class teacher until the end of the school day.

Policy Statements

Education –pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff will reinforce e-safety messages across the curriculum. The e-safety curriculums is broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- ✓ A planned e-safety curriculum is provided as part of Computing and part of the schools wider curriculum.
- ✓ Key e-safety messages will be reinforced as part of a planned programme.
- ✓ Pupils will be taught in all lessons to be critically aware of the materials / 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
- ✓ Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- ✓ Staff will act as good role models in their use of digital technologies the internet and mobile devices
- ✓ 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 will be vigilant in monitoring the content of the websites the young people visit.
- ✓ It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and 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. Any request to do so, will be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- ✓ Curriculum activities
- ✓ Letters, newsletters, web site
- ✓ Parents / Carers evenings / sessions
- ✓ High profile events / campaigns e.g. Safer Internet Day
- ✓ Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- ✓ A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- ✓ All new staff should receive e-safety training, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- ✓ The E-Safety Coordinator will receive regular updates through attendance at external training events (eg. LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- ✓ This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- ✓ The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

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

- ✓ Attendance at training provided by the Local Authority.
- ✓ Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- ✓ Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- ✓ There will be regular reviews and audits of the safety and security of academy technical systems
- ✓ Servers, wireless systems and cabling must be securely located and physical access restricted
- ✓ All users will have clearly defined access rights to academy technical systems and devices.
- ✓ All users will be provided with a username and secure password by technical support team. Users are responsible for the security of their username and password and will be required to change their password every year.
- ✓ The “master / administrator” passwords for the academy ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe)

- ✓ The technical support team is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- ✓ Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- ✓ Netsweeper is the main filtering system used by the academy alongside Visigo (monitored by Walsall ESafety team as of April 2018) that is used to monitor internet usage by staff and children.
- ✓ The school has provided enhanced / differentiated user-level filtering.
- ✓ Academy technical staff regularly monitors and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- ✓ An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. Follow the schools safeguarding procedures.
- ✓ 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 school infrastructure and individual workstations are protected by up to date virus software.
- ✓ An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- ✓ Identified staff have permission to download executable files and installing programmes on school devices. Other staff need to seek permission.
- ✓ All staff are provided with a removable memory stick which is encrypted to ensure all personal data is secure. (e.g. memory sticks / CDs / DVDs) by users on school devices. Hard drives will be given to provide space for storing planning information. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- ✓ Staff to only use school email addresses given to share information.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet as part of their digital footprints and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- ✓ When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- ✓ In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- ✓ Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policy that images are deleted or downloaded as soon as possible and the device must contain a secure password. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- ✓ Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- ✓ 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.
- ✓ Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- ✓ Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (See appendix AUP children)
- ✓ Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 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.

The academy must ensure that:

- ✓ It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- ✓ Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- ✓ All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- ✓ It has a Data Protection Policy (See appendix Data protection)
- ✓ It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- ✓ Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs) schools business manager.
- ✓ Risk assessments are carried out
- ✓ It has clear and understood arrangements for the security, storage and transfer of personal data
- ✓ Data subjects have rights of access and there are clear procedures for this to be obtained
- ✓ There are clear and understood policies and routines for the deletion and disposal of data
- ✓ There is a procedure for reporting, logging, managing and recovering from information risk incidents (CPOMS)
- ✓ There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- ✓ There are clear procedures about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office. In conjunction with the email facilities provided staff are given additional storage space through their OneDrive accounts where staff are able to store information safely.

Staff must ensure that they:

- ✓ 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.
- ✓ Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- ✓ The data must be encrypted and password protected

- ✓ 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 (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to school		X						X And handed in
Use of mobile phones in lessons				X				X
Use of mobile phones in social time (Away from staff)	X							X
Taking photos on mobile phones / cameras (personal)				X				X

Use of other personal mobile devices eg 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

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

- ✓ Users should be aware that email communications are monitored. Staff and pupils should therefore use only the academy email service to communicate with others when in school, or on academy systems
- ✓ Users must immediately report, to the nominated person – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- ✓ Any digital communication between staff and pupils or parents / carers (email, etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- ✓ Whole class / group email addresses may be used at KS1.
- ✓ Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- ✓ Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

- ✓ All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
- ✓ The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:
- ✓ Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- ✓ Clear reporting guidance, including responsibilities, procedures and sanctions
- ✓ Risk assessment, including legal risk
- ✓ School staff should ensure that:

- ✓ No reference should be made in social media to pupils, parents / carers or school staff
- ✓ They do not engage in online discussion on personal matters relating to members of the school community
- ✓ Personal opinions should not be attributed to the academy or local authority
- ✓ Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

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

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated 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					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business				X		
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X		
Infringing copyright				X		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X		
Creating or propagating computer viruses or other harmful files				X		
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X		
On-line gaming (educational)				X		
On-line gaming (non educational)				X		

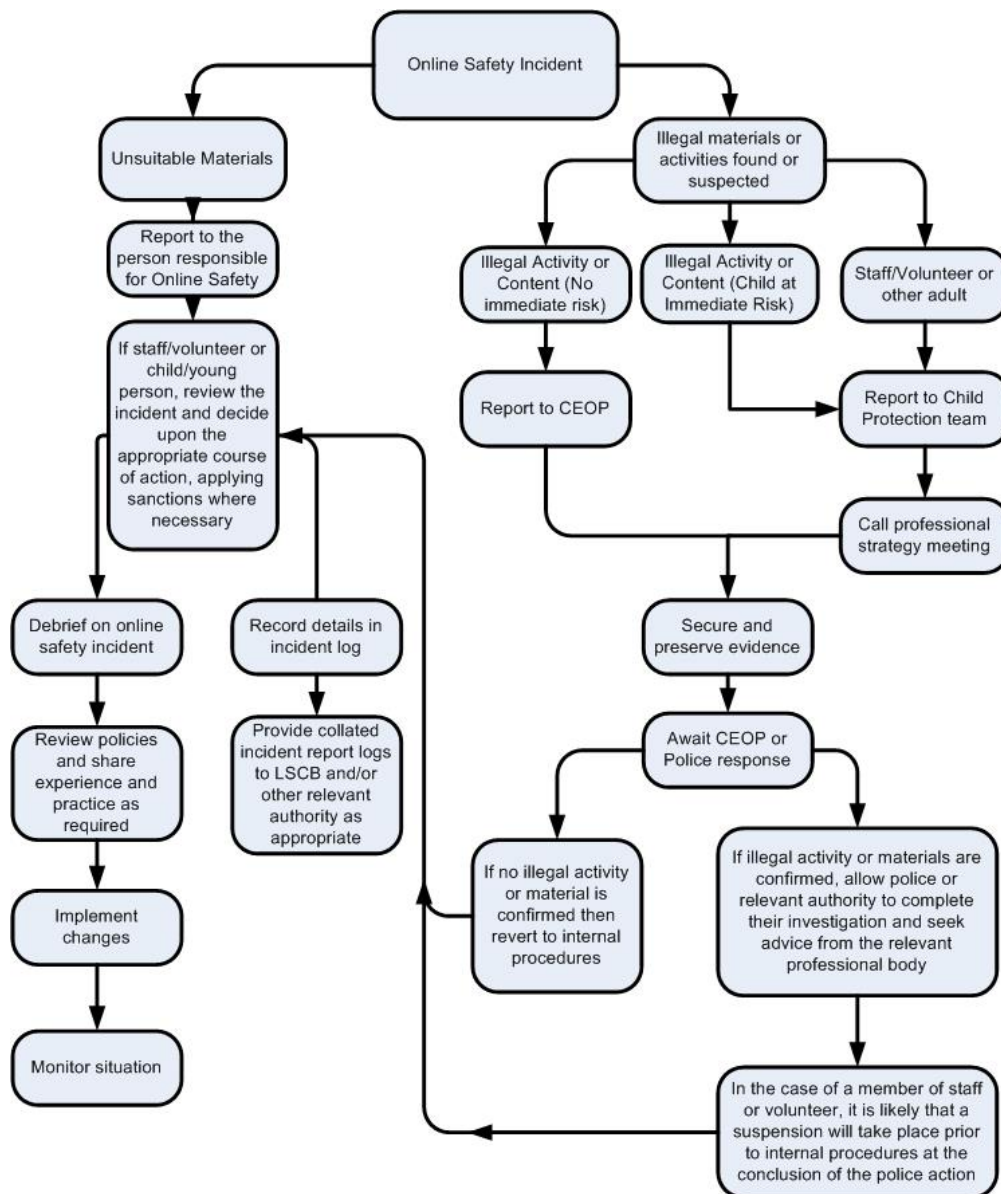
On-line gambling				X	
On-line shopping / commerce				X	
File sharing				X	
Use of social media				x	
Use of messaging apps				x	
Use of video broadcasting eg Youtube		x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- ✓ Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- ✓ Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- ✓ It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- ✓ Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- ✓ Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - ✓ Internal response or discipline procedures
 - ✓ Involvement by Local Authority
 - ✓ Police involvement and/or action
- ✓ If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - ✓ incidents of 'grooming' behaviour
 - ✓ the sending of obscene materials to a child
 - ✓ adult material which potentially breaches the Obscene Publications Act
 - ✓ criminally racist material
 - ✓ other criminal conduct, activity or materials
- ✓ Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Academy Actions & Sanctions

It is more likely that the academy 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

Incidents:	Refer to class teacher	Refer to Head Teacher	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).		X	X					
Unauthorised use of non-educational sites during lessons	X	X		X		X	X	
Unauthorised use of mobile phone / digital camera / other mobile device		X			X		X	X
Unauthorised use of social media / messaging apps / personal email		X			X	X	X	X
Unauthorised downloading or uploading of files		X		X	X	X	X	X
Allowing others to access academy network by sharing username and passwords	X	X		X	X		X	X
Attempting to access or accessing the academy network, using another pupil's account	X	X		X	X		X	X
Attempting to access or accessing the academy network, using the account of a member of staff	X	X		X	X		X	X
Corrupting or destroying the data of other users		X		X	X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X		X	X
Continued infringements of the above, following previous warnings or sanctions		X			X		X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X		X	X
Using proxy sites or other means to subvert the academy's filtering system		X	X	X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X		X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X		X	X		X	X

Staff

Actions / Sanctions

Incidents:	Refer to Head Teacher	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).	X	X	X		X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X					X
Unauthorised downloading or uploading of files	X			X	X		
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	X			X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X				X		
Deliberate actions to breach data protection or network security rules	X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X						X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X					X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X					X
Actions which could compromise the staff member's professional standing	X	X					X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X					X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X	X			X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X						X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X

Pupil Acceptable Use Agreement

Academy Policy

Digital technologies have become integral to the lives of children and young people, both within the academy and outside. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

If for any reason you do not wish your child's work or photograph to be displayed on the schools website could you please let me know in writing. Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

Yours sincerely,



Acceptable Use Policy

- I will ask a teacher or suitable adult if I want to use the computer.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment that I use.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the academy systems and devices.

Required Signature PARENTS / CARERS

I have read this Acceptable Use Policy **and I have discussed this with my child.**

I agree for my child _____ Class _____
to use the Internet in accordance with the school guidelines.

Signed _____ (Parent/Carer)

Signed _____ (Pupil)

Date: _____

Pupil Acceptable Use Agreement

Academy Policy

Digital technologies have become integral to the lives of children and young people, both within the academy and outside. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

If for any reason you do not wish your child's work or photograph to be displayed on the schools website could you please let me know in writing. Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

Yours sincerely,



Head Teacher

Acceptable Use Policy

- I understand that the school will monitor my use of the computer/iPad.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of 'stranger danger' when I am communicating online.
- I will not tell anyone my personal information about myself or others online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the academy systems and devices.

Required Signature PARENTS / CARERS

I have read this Acceptable Use Policy **and I have discussed this with my child.**

I agree for my child _____ Class _____
to use the Internet in accordance with the school guidelines.

Signed _____ (Parent/Carer)

Signed _____ (Pupil)

Date: _____

Acceptable Use Policy for staff

- I understand that the school will monitor my use of the computer/iPad.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour.
- I understand if I fail to comply with this policy I will be subject to disciplinary action.
- Staff are reminded to refer to the code of conduct regarding the use of computers.

Required Signature

I have read this Acceptable Use Policy and agree to uphold the agreement.

Signed _____ (Print name)

Signed _____ (Signature)

Date: _____

Woodlands Academy of Learning



Behaviour Policy

SAFEGUARDING CHILDREN

Behaviour Policy

This policy sets out the expectations of behaviour at Woodlands Academy. As a caring community, we aim to create an environment which encourages and reinforces good behaviour and the fostering of positive attitudes.

We have high expectations for good behaviour throughout the school and at all times during the school day. This is closely linked to the ethos and Mission Statement of our school we feel it is vital that the school adopts and maintains a consistent approach to behaviour at all times and by all members of the school community. This policy also links to the school Anti-bullying policy.

Aims

- To promote a positive ethos in the school through encouraging a shared understanding of the values which underpin our school ethos
- To create a consistent environment that expects, encourages and recognises good behaviour and one in which everyone feels happy and safe
- To help pupils develop self-respect, self-control and accountability for their own behaviour
- To further promote self-esteem through success, positive relationships and awareness of how our behaviour impacts on ourselves and others
- To encourage the partnership between home and school

We are a caring inclusive school and aim for every member of our school community to feel valued and respected. We all have the right to be treated well and fairly. The school behaviour policy is therefore designed to encourage the way in which all members –pupils, staff, parents and governors, can work together in a mutually supportive way. It aims to promote an environment where everyone feels safe and secure and where the health and well-being of individuals is paramount. Relationships should be based on fairness, honesty, respect, courtesy and consideration.

Our behaviour policy focuses on positive behaviour management, promoted and supported in the following ways:

- A carefully planned curriculum
- Effective classroom management
- Adult role-modelling
- Whole school behaviour management plan
- Playtime and lunchtime provision (structured playground games)
- Personalised programmes/ support from outside agencies

Curriculum and Classroom Management

Alongside positive relationships, we are aware that good classroom organisation and effective teaching methods are key to good behaviour and that the provision of a high quality curriculum through interesting and challenging activities influences behaviour. A welcoming and secure classroom environment gives clear messages to the children about the extent to which they and their efforts are valued.

Learning environments will be organised to promote and develop independence and individual initiative, whilst minimising disruption and uncertainty. This includes the arrangement of furniture and suitable access to resources and learning materials.

Displays aim to be current, lively and help develop self-esteem through demonstrating the value of every individual's contribution.

Staff Responsibilities

- To role model good behaviour and positive relationships
- To create a positive climate with realistic expectations
- To emphasise the importance of values and being valued
- To provide an effective learning and teaching environment
- To encourage positive relationships based on kindness, empathy and respect
- To ensure fair treatment for all regardless of ability, age, gender, race or preconceptions
- Show appreciation of the efforts and contributions of everyone

All adults in school including lunchtime supervisors, parent helpers and site staff etc, are responsible for the modelling of good behaviour, positive relationships and dealing with incidents around school.

Behaviour Management Plan

Our behaviour management plan is based on initial respect.

Everyone in our school has the right to.....

- learn
- be respected
- be safe
- be happy

Therefore everyone is expected to follow these whole school rules:

- We will always use commonsense, courtesy and consideration
- We will always try our best and allow others to do the same.
- We will show respect by looking after ourselves, others and school property.
- We will listen and follow adult instructions.

At the start of the school year, classes will negotiate and agree a small number of additional positive rules as part of a class charter or code of conduct, in order to promote a positive and safe learning environment. All rules will be clearly displayed in the classroom and referred to regularly.

Recognition

We aim to create a healthy balance between rewards and consequences with both being clearly explained and specified. Pupils should learn to expect recognition for positive behaviour and fair and consistently applied consequences for inappropriate behaviour. All systems are flexible to take account of individual circumstances. The emphasis is on positive behaviour management through REWARDS and PRAISE, which should be given whenever possible for both work and behaviour. Recognition and tangible rewards are given on individual, group and whole class levels in order to promote a sense of both individual and corporate responsibility.

- Praise and positive individual or group recognition
- Stickers – either worn by child, or collected on a chart or card
- Positive recognition to parents at the end of the session/ day
- House points awarded
- Showing work to another adult/ class/ Headteacher
- Certificates (presented in assembly)
- Collective whole class rewards
- Diddy dots
- Stamp charts
- ‘You’re a star’

House point system

All children belong to a house group, brothers and sisters in the same house group, in which they remain. House points can be awarded by any adult in school. House points are high in value and are awarded for actions/ behaviour that are above and beyond what is normally expected. Each week the children add their merits to a collective score for their house (counted by school council members) and this is displayed in the hall. The winning house gets to choose their reward at the end of the year.

Dealing with unacceptable behaviour

Teachers should employ a variety of strategies to manage the behaviour of their children, for example: visual displays, avoidance/ distraction techniques etc. Avoidance/ distraction techniques can be: verbal reminder, moving the child, physically moving closer, acknowledging look to the child, PIP (Praise in Public), RIP (Reprimand in Private). These intervention/ distraction strategies should be used to defuse the behaviour, if it continues a warning should be given. The child should be made aware that being given a warning is a very serious issue.

Despite positive responses as a means to encouraging good behaviour, it may be necessary to employ a number of consequences if unacceptable behaviour escalates to enforce the school rules, and to ensure a safe and positive learning environment.

We operate a hierarchy of corrective interventions and consequences, which are age appropriate, working from the least to most intrusive. The hierarchy is made explicit to the children as is the link between the behaviour and consequence. A variety of low level intervention strategies are used initially, such as non-verbal signals, reminders and close adult proximity to re-direct and encourage children to stay on track. If the inappropriate behaviour persists, then the consequences are presented to the child as a choice to help teach children that they are responsible for their own behaviour.

Within the classroom, the following consequences will be used for increasingly inappropriate or continued disruptive behaviour, however extreme behaviour, such as physical aggression towards others, will result in immediate removal from the classroom and/ or being sent to the Sycamore Suite and the Head teacher will be informed.

The emphasis at any stage is on the child being re-engaged in the lesson and their learning as soon as appropriate.

Stage 1-3- teacher level, mainly low level behaviours

Consequences

Stage 1: Verbal reminder of the expected behaviour/ school rule

Choice presented to child – You can choose to or you can choose to

..... If you choose to then you will have time out.

Stage 2: Time out within classroom to reflect on their behaviour and what they should have done differently. (3-5 minutes for KS1, 5-10 minutes for KS2) Name recorded on class tracker sheet.

Choice presented to child – You can choose to or you can choose to

..... If you choose to then there will be a further consequence.

Stage 3: Time out outside the classroom or in another class, with work- recorded on Tracker sheet- child to reflect on their choice of behaviour and what they should do differently

Repeated incidents or reaching stage 3 regularly will be reported to parents at the end of the day or as soon as possible, either in person, by letter or phonecall by the teacher

Choice presented to child – You can choose to or you can choose to

..... If you choose to then there will be further consequence.

Stage 4: Unacceptable/ disruptive, serious behaviour

Sent out with orange slip detailing behaviours (including mid level behaviours)- This is extremely serious high level behaviour and such behaviours cannot always be defined- staff to use their common sense when placing a child at this stage.

Time out working away from class, with appropriate work, for one session, in Sycamore Suite

Parent informed by phone or letter by learning support coordinator

Monitor behaviour/ individual behaviour

Stage 5: Severe behaviour

Extremely unacceptable behaviour will be reported to the Headteacher, Deputy Headteacher or Assistant Headteacher immediately. A letter will be sent home or a phone call made to the parents the same day. For continual unacceptable behaviour or in case of serious verbal or physical aggression the child may be excluded internally from their class. This may also lead to a fixed-term exclusion, or on rare occasions, may take the form of a permanent exclusion (see 'fixed-term and permanent exclusions' below).

Following an incident of unacceptable behaviour, adults will have a private conversation with the child when they are calm, focusing on 'repair' and 'putting it right' to ensure a sense of closure. It will also focus on the child taking responsibility for their own actions and may involve the use of prompt questions, such as: How did you make other people feel? Is there anything you wish you'd done differently? What can you do to put it right? Is there anything I can help you with so it doesn't happen again?

Use of Reasonable Force

All members of school staff have a legal power to use reasonable force to prevent pupils:

- Committing an offence
- Injuring themselves or others
- Damaging property
- Disturbing good order, discipline and learning in the classroom, eg failure to leave the classroom when requested to do so.

Force is never used as a punishment, but is used to bring pupils under control or to restrain them.

Reasonable adjustments will be made for those children with a disability and/or Special Educational Needs.

Parents will be informed and a 'Physical intervention Recording form' will be completed and a 'Positive Handling Plan' will also be completed for that child. This will be signed by all staff who intervened, the headteacher, pupil and parent.

Playtimes and Lunchtimes

At play and lunchtimes we aim to provide a range of activities to engage children in positive play with their peers, with the focus on co-operative play, good communication and teamwork. KS2 and KS1 children have the option of playing indoors in the play room at lunchtime.

If problems between children arise, the emphasis is on peaceful problem solving and conflict resolution. Consequences are 'time out' to calm down and think about their actions or if the behaviour continues children are sent to the Sycamore Suite and are excluded off the playground. Children are recognised for positive behaviour at play and lunchtimes through

verbal praise and public recognition, passing the good news and incidents onto class teachers and other adults and the awarding of house points.

.

Consequences

At play and lunchtimes there is a three stage hierarchy of corrective interventions and consequences.

Stage 1: (1st Yellow Card)- Rule/ expected behaviour reminder

Choice presented to child – You can choose to or you can choose to

..... If you choose to then you will have time out.

Stage 2: (2nd Yellow Card)- Timeout for 5 minutes – child to stand next to and follow adult or stand by wall. Incident recorded in the incident book.

Choice presented to child – You can choose to or you can choose to

..... If you choose to then there will be a further consequence.

Stage 3: (Red Card)- Timeout in Sycamore Suite for remainder of play or lunchtime

Incident recorded in the lunchtime incident book and Sycamore Suite incident book.

Class teacher, Headteacher/ deputy/ assistant head informed.

If stage 3 reached more than once then parents to be informed.

Once again, adults will follow an incident of unacceptable behaviour with a private conversation focusing on 'repair' to ensure a sense of closure, and on the child taking responsibility for their own actions.

In the event of extremely unacceptable behaviour or persistent disruptive behaviour at play and lunchtimes, then a child will be brought inside off the playground straight away and may be excluded from play and lunchtimes for a fixed period.

Children's Responsibilities

Children are expected to follow the school rules and classroom codes of conduct, showing respect for the rights and needs of all adults and other children in our school community. The school council will play an important role in communicating and reviewing aspects of the behaviour policy.

Parents' Responsibilities

Parents have a vital role to play in their children's education – supporting their child's learning and working in partnership with the school. We are very conscious of the importance of good communication between home and school. Thus, the school aims to work collaboratively with parents, so children receive consistent messages about how to behave at home and at school. It is important for all adults on school site, including parents, to model positive behaviour at all times and in particular in their interactions with each other.

We display the school's rules, rewards and consequence systems and explain them in the school prospectus. We have a Home/School agreement which is signed by pupils, parents and teachers. We expect parents to read these and support them. If a member of school staff has concerns about a child's welfare or behaviour, parents will be contacted as outlined above. If the school has to use reasonable consequences as the result of unacceptable behaviour, parents should support the actions of the school. If parents have a concern about an incident that has happened in school, they should initially contact the class teacher. The Deputy and Assistant Head may then be involved, then the Headteacher and, if the concern remains, they should contact the school governors.

We expect parents to behave in a reasonable and civilised manner towards all school staff, and professionals, and that issues will be dealt in an atmosphere of trust and mutual respect. Incidents of verbal or physical aggression to staff by parents/guardians/carers of children in the school will be reported immediately to the Headteacher and/or Governors who will take appropriate action in line with Local Authority policy.

Special Educational Needs

We recognise that for a small number of children, whose behaviour is beyond the whole school rewards and consequences system, a more personalised approach may be necessary in order to support them in developing the ability to regulate their own behaviour. They may have an individual behaviour plan agreed between the pupil, staff and parents. The support of outside agencies will also be sought where appropriate, in particular Educational Psychologist and other health agencies.

Fixed term and Permanent exclusions

Extreme behaviour or persistent disruptive and challenging behaviour may lead to a pupil exclusion. Only the Headteacher (or the acting Headteacher) has the power to exclude a child from school. The Headteacher may exclude a pupil for one or more fixed periods, for up to 45 days in any one school year. The Headteacher may also exclude a pupil permanently. It is also possible for the Headteacher to convert a fixed-term exclusion into a permanent exclusion, if the circumstances warrant this.

If the Headteacher excludes a child, she informs the parents as soon as possible, giving reasons for the exclusion. At the same time, the Headteacher makes it clear to the parents

that they can appeal against the decision to the Governing Body and how to do so through the letter of exclusion.

The Headteacher informs the Local Authority (LA) and the Governing Body about any permanent exclusion or fixed-term exclusions. The Governing Body itself cannot either exclude a child or extend the exclusion period made by the Headteacher. However, the Governing Body has a discipline committee whose role is set out in strict guidelines whenever a child is excluded from school.

Recording, monitoring and evaluating behaviour

Behaviour in school will be recorded through tracker sheets, behaviour books and lunchtime incident book and on Facility (school MIS system). Progress towards individual targets will be recorded on individual behaviour/ education plans and positive handling plan. The Management Team and learning support coordinator will monitor behaviour and evaluate the impact of this policy through the records listed above, through informal observations, comments from formal lesson observations and discussion with pupils, staff and parents.

This policy will be reviewed annually, with opportunities for consultation with staff, pupils and parents.

January 2016

Behaviour Management Plan 2016

Implementation of consequences requires **common sense** and an understanding **of context and the individual**. Children to be made aware of the seriousness of being on the tracker and all behaviour strategies have been implemented before issuing the first warning.

Low level behaviour			
Examples of behaviour	Consequence	Stage	Staff

<ul style="list-style-type: none"> • Calling out • Talking when others are talking • Being disrespectful to staff and other children • Failure to follow instructions • Poor display of common courtesies • Inappropriate play • Failure to follow school/class rules • Refusal to complete work • Inappropriate language 	<p>Verbal warning: Present choice to child e.g, “you can choose to follow the rules but if you choose not to then you will have a warning and go on the tracker.”</p> <p>1-Warning: Warning circled on Tracker. Reminder of class/ school rules and expected behaviour. Present choice to child e.g, “you can choose to follow the rules but if you choose not to then you will have time out.”</p> <p>2-Time out: Number 2 circled on tracker and time out in class. Again present choice to child.</p> <p>3-Time out in another class- Number 3 circled on tracker and child sent to another class, with work, for remainder of session. Present choice to child.</p> <p>Parent/ carer informed if reaching stage 3 regularly.</p>	<p>1-3</p>	<p>Teacher or TA/LSA</p> <p>Teacher or TA/LSA</p> <p>Teacher</p> <p>Teacher</p> <p>Teacher</p>
--	---	-------------------	--

Mid- Level Behaviour			
Examples of Behaviour	Consequence	Stage	Staff
<ul style="list-style-type: none"> • Wilful damage to other peoples/ schools property • Continuous low level behaviour within one day • Physical contact with intent to hurt • Racist, homophobic or sexist language 	<p>Removed from class to Mrs Graham or a member of the SMT, with an orange slip and appropriate work for one session Or Internally excluded out of class.</p> <p>Communication to parents- verbally or by letter if appropriate.</p>	<p>4</p>	<p>Class teacher, Mrs Graham, SMT</p> <p>Class teacher, Mrs Graham, SMT</p>
Severe Behaviour			
Examples of behaviour	Consequence		Staff

Woodlands Academy of Learning



Data Protection Policy

Contents:

[Statement of intent](#)

1. [Data controller](#)
2. [Fair processing](#)
3. [Data security](#)
4. [Subject consent](#)
5. [Rights to access information](#)
6. [Publication of information](#)
7. [CCTV and photography](#)
8. [Data retention](#)
9. [Challenges and compensation](#)

Statement of intent

Woodlands Academy of Learning is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the Data Protection Act 1998.

The academy may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially social services.

This policy is in place to ensure all staff and governors are aware of their responsibilities under the Data Protection Act and outlines how Woodlands Academy of Learning complies with the following core principles of the Act:

- Data must be processed fairly and lawfully.
- Data must only be acquired for one or more lawful purposes and should not be processed for other reasons.
- Data must be adequate, relevant and not excessive.
- Data must be kept accurate and up-to-date.
- Data must not be kept for longer than is necessary.
- Data must be processed in accordance with the data subject's rights.
- Appropriate measures must be taken to prevent unauthorised or unlawful access to the data and against loss, destruction or damage to data.
- Data must not be transferred to a country or territory unless it ensures an adequate level of protection for the rights of the subject.

Organisational methods for keeping data secure are imperative, and Woodlands Academy of Learning believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Data controller

- 1.1. The academy, as the corporate body, is the data controller.
- 1.2. The governing body of Woodlands Academy of Learning therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.
- 1.3. The school business manager will deal with the day-to-day matters relating to data protection.
- 1.4. Therefore, the school business manager is responsible for processing personal information on the academy's behalf. The security of the personal information is covered in a written agreement/formal contract between the academy and the school business manager.

2. Fair processing

- 2.1. Woodlands Academy of Learning recognises that its staff members and pupils need to know what the academy does with the information it holds about them.
- 2.2. Parents will receive a copy of this Data Protection Policy upon registration of their child at Woodlands Academy of Learning as well as an overview of the information that the academy will keep about their child.
- 2.3. Woodlands Academy of Learning issues a general privacy notice, detailing the purposes for which personal data collected by the academy will be used, before obtaining or with a request for any personal information.
- 2.4. If personal details are being recorded for a specific purpose, a specific privacy notice may be issued.
- 2.5. Personal information is only made available to staff and governors who need that particular information to do their jobs, and is only made available at the time that it is needed.
- 2.6. All staff members, including members of the governing body will receive training in their responsibilities under the Data Protection Act, and guidance on confidentiality of personal information, as part of their HR induction.
- 2.7. The training will be reinforced at regular intervals throughout their employment/term as governor, e.g. on inset days.
- 2.8. Staff members and parents are responsible for checking that any information that they provide to the academy in connection with their employment or in regard to a registered pupil is accurate and up-to-date.
- 2.9. The academy cannot be held accountable for any errors unless the employee or parent has informed the academy about such changes.
- 2.10. The school business manager is responsible for monitoring fair processing controls on a regular basis.

3. Data security

- 3.1. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
- 3.2. Confidential paper records should not be left unattended or in clear view anywhere with general access.
- 3.3. Computerised data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- 3.4. Where data is saved on removable storage or a portable device, the device must be kept in a locked filing cabinet, drawer or safe when not in use.
- 3.5. Memory sticks should not be used to hold personal information unless they are password-protected and fully encrypted.
- 3.6. All electronic devices must be password-protected to protect the information on the device in case of theft.

- 3.7. Where possible, Woodlands Academy of Learning enables electronic devices to allow the remote blocking/deletion of data in case of theft.
- 3.8. Staff and governors should not use their personal laptops or computers for academy purposes.
- 3.9. All necessary staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- 3.10. Emails containing sensitive or confidential information should be password-protected if there are insecure servers between the sender and the recipient.
- 3.11. Circular emails to parents should be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 3.12. When sending confidential information by fax, staff must check that the recipient is correct before sending.
- 3.13. Woodlands Academy of Learning uses Squirrel Mail and the DFE Secure Access site secure sending systems.
- 3.14. Where personal information that could be considered private or confidential is taken off the school premises, either in electronic or paper format, staff must take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises must accept full responsibility for the security of the data.
- 3.15. Before sharing data, all staff must ensure:
 - They are allowed to share it.
 - That adequate security is in place to protect it.
 - Who will receive the data has been outlined in a privacy notice.
- 3.16. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information must be supervised at all times.
- 3.17. The physical security of the school buildings and storage systems, and access to them, is reviewed termly. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- 3.18. Woodlands Academy of Learning takes its duties under the Data Protection Act seriously and any unauthorised disclosure may result in disciplinary action.

4. Subject consent

- 4.1. Woodlands Academy of Learning understands that subjects have certain legal rights to their personal data, which will be respected.
- 4.2. The academy will not process personal data without the consent of the subject, although the processing of data will sometimes be necessary for:
 - The performance of a contract to which the subject is party to, or the steps taken with a view to entering a contract.

- Compliance with a legal obligation to which the academy is subject.
 - The administration of justice, legal functions of persons or departments, or functions of a public nature exercised in the public interest.
 - The purposes of legitimate interests of the academy, unless the decision prejudices the rights, freedoms or legitimate interests of the subject.
- 4.3. Staff members of the academy will be working in close contact with children. Disclosure and Barring Service (DBS) checks will therefore be made a condition of employment in order to ensure that potential employees do not pose a threat or danger.
- 4.4. Sensitive data, including: information relating to a subject's racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health; their sex life; or the commission of any offence, can only be processed with the explicit consent of the subject.
- 4.5. Sensitive data will only be processed if:
- It is necessary to protect the subject's vital interests.
 - It is carried out in the course of legitimate activities by a not-for-profit body or association with appropriate safeguards.
 - It is necessary for the administration of justice or other legal purposes.
 - It has been ordered by the Secretary of State.
 - It is necessary to prevent fraud.
 - It is necessary for medical purposes.
 - It is necessary for equality reasons.
 - It was made public deliberately by the data subject.

5. Rights to access information

- 5.1. All staff members, parents of registered pupils and other users are entitled to:
- Know what information the academy holds and processes about them or their child and why.
 - Understand how to gain access to it.
 - Understand how to keep it up-to-date.
 - Understand what the academy is doing to comply with its obligations under the Data Protection Act.
- 5.2. All staff members, parents of registered pupils and other users have the right, under the Data Protection Act, to access certain personal data being held about them or their child.
- 5.3. Personal information can be shared with pupils once they are old enough, although this information can still be shared with parents/guardians.
- 5.4. The academy aims to comply with requests for access to personal information as quickly as possible, but will ensure that it meets its duty under the Data Protection Act to provide it within 40 working days.
- 5.5. Woodlands Academy of Learning will comply with its obligations under the Data Protection Act to provide subjects access to personal information.
- 5.6. All subject access requests must be kept in a log that requires formal consideration.

- 5.7. The academy may charge a fee of £10 or more on each occasion that access is requested.
- 5.8. The academy is not obliged to provide unstructured personal data if the administrative cost is deemed to exceed the limit of £450 as contained in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.
- 5.9. Woodlands Academy of Learning is not obliged to supply access to information unless it has received:
 - A request in writing.
 - The fee required.

6. Publication of information

- 6.1. Woodlands Academy of Learning will publish a publication scheme on its website outlining classes of information that will be made routinely available, including:
 - Policies and procedures..
 - Annual reports.
 - Financial information.
- 6.2. Classes of information specified in the publication scheme will be made available quickly and easily on request.
- 6.3. Woodlands Academy of Learning will not publish any personal information, including photos, on its website without the permission of the affected individual.
- 6.4. When uploading information to the school website, staff must be considerate of any metadata or deletions which could be accessed in documents and images on the site.

7. Photography and Videos

- 7.1. Woodlands Academy of Learning understands that recording images of identifiable individuals constitutes processing personal information, so must be done in line with data protection principles.
- 7.2. The academy will always indicate its intentions for taking photographs of pupils and retrieve permission before publishing them.
- 7.3. If the academy wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent/guardian of the pupil.
- 7.4. Precautions, as outlined in the Photography Policy, will be taken when publishing photographs of pupils, in print, video or on the website.
- 7.5. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the Data Protection Act.

8. Data retention

- 8.1. The Data Protection Act states that data should not be kept for longer than is necessary.
- 8.2. In the case of Woodlands Academy of Learning, unrequired data will be deleted as soon as practicable.
- 8.3. Some educational records relating to a former pupil or employee of the academy may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.
- 8.4. Records of DBS checks will be destroyed immediately, although the date that the check was made will be retained in the academy's file.
- 8.5. Paper documents must be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

9. Challenges and compensation

- 9.1. Woodlands Academy of Learning understands that staff members and the parents of registered pupils have the right to prevent the processing of personal data if it is likely to cause damage or distress.
- 9.2. Individuals with concerns related to the processing of personal data should provide the school business manager with written notice.
- 9.3. If the school business manager receives a written notice asking them to cease or not to begin processing specified data, they must reply in writing within 21 days detailing:
 - Their compliance or their intent to comply; or
 - Their reasons for considering the subject's written notice unjustified and the extent to which they have complied, or intend to comply, with the request.
- 9.4. Data subjects reserve the right to take their concerns to a court of law and will be entitled to compensation if it is judged that the academy contravened the provisions of the Data Protection Act.
- 9.5. Individuals who are not the subject of the data, but suffer damage as a result of the contravention, are also entitled to compensation.
- 9.6. It is the individual's own responsibility to take action for compensation if loss of personal data causes them damage.
- 9.7. The academy will immediately rectify, block, erase or destroy any data that a court of law judges to have contravened the requirements of the Data Protection Act.

Useful links for parents

Care for the family www.careforthefamily.org.uk

Know It All www.childnet.com/KIA

Internet Watch Foundation www.iwf.org.uk

Internet Safety Zone www.internetsafetyzone.com

Get Safe Online www.getsafeonline.org

Think U Know www.thinkuknow.co.uk/parents

Safer Internet Centre <http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers>

NSPCC <https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>