Woodlands Academy of Learning

Online Safety Policy
October 2020

Development / Monitoring / Review of this Policy

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

- ✓ Mrs Newton Head teacher
- ✓ Miss S Harvey Online safety Lead
- ✓ Mrs J Graham Deputy Safeguarding lead
- ✓ Mrs L Garcha – Assistant Head/ Maths Leader
- ✓ Mr Ian Whitehouse –Governor
- ✓ Nicola Rudge – Local Authority Online safety advisor

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

Schedule for Development / Monitoring / Review

This online safety policy was approved by the *Governing Body*	Yes
The implementation of this online safety policy will be monitored by the:	*Miss S Harvey – Online safety Lead, Link governor Ian Whitehouse – safeguarding governor*
Monitoring will take place at regular intervals:	*Half termly*
The *Governing Body* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*May 2021*
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	May 2021
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Mrs T Newton – Head teacher* *Mrs J Graham – Deputy Safeguarding Lead* *Mrs C Macpherson – Deputy Safeguarding Lead*

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 (Walsall monitoring service using Smoothwall Monitor)
- ✓ 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 Computing 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 online 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 online safety behaviour that take place out of school.

Roles and Responsibilities

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

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 Co-ordinator
- ✓ regular monitoring of online 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 online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online 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 online safety allegation being made against a member of staff. (See Safeguarding and Child Protection Policy)
- ✓ The Head teacher is responsible for ensuring that the Online safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online 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 online 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 Smoothwall Monitor when sent to school.
- ✓ 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.

Online safety Coordinator

- ✓ Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ✓ Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place (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 online safety incidents and creates a log of incidents to inform future online safety developments.
- ✓ Meets regularly with Online 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 online safety technical information in order to effectively carry out their online 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 online safety matters and of the current academy online 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/ Online 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
- ✓ Online safety issues are embedded in all aspects of the curriculum and other activities
- ✓ Pupils understand and follow the online safety and acceptable use policies
- ✓ 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 online 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 online-bullying.
- ✓ Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's Online 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 and pupils continue to be trained each year in order to support Online safety at the academy.

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 online safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good online 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 online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- ✓ A planned online safety curriculum is provided as part of Computing and part of the schools wider curriculum.
- ✓ Key online safety messages will be reinforced as part of a planned programme using Education for a connected world statements as a starting point.
- ✓ 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 online 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 online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

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

Training – Governors

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

- ✓ Attendance at training provided by the 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 online 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 Computing 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 Smoothwall Monitor (monitored by Walsall Online monitoring team) 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" (e.g. 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 in 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			
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 And han ded 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 online 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:

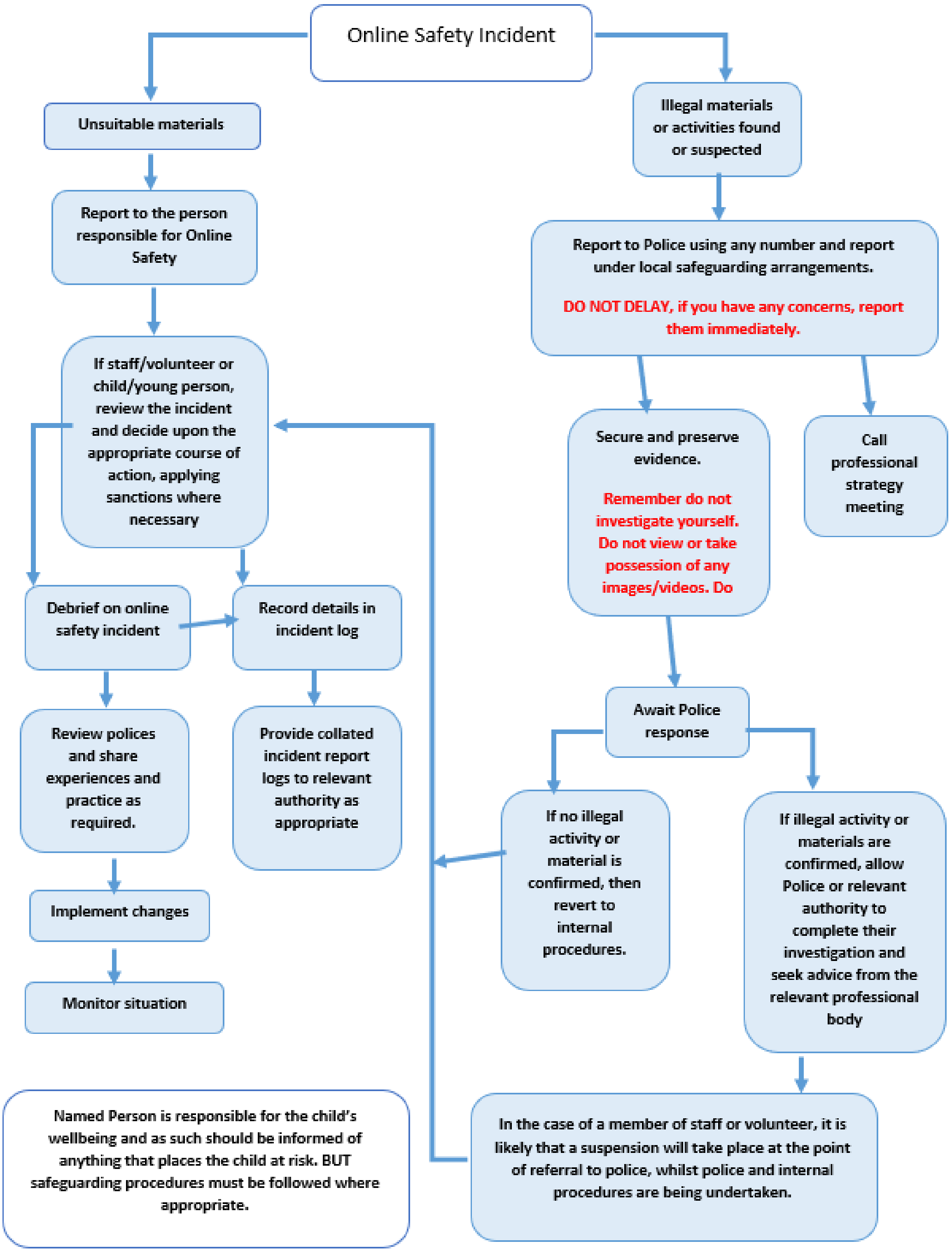
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

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 e.g. 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	x	x	x	x	x	x	x

and failing to report the incident							
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

Woodlands
Academy of Learning

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: ____________________

Woodlands Academy of Learning

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**

• 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	**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." **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." **2-Time out:** Number 2 circled on tracker and time out in class. Again present choice to child. **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. **Parent/ carer informed if reaching stage 3 regularly.**	**1-3**	Teacher or TA/LSA Teacher or TA/LSA Teacher Teacher Teacher

Mid- Level Behaviour			
Examples of Behaviour	**Consequence**	**Stage**	**Staff**
• 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	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. Communication to parents- verbally or by letter if appropriate.	**4**	Class teacher, Mrs Graham, SMT Class teacher, Mrs Graham, SMT
Severe Behaviour			
Examples of behaviour	**Consequence**		**Staff**

• Severe physical aggression • Un-provoked aggression • Reaching stage 4 on a regular basis • Verbal aggression including use of very inappropriate language • Constant open defiance of instructions • Racist abuse • Homophobic abuse • Sexist abuse • Theft • Carrying a weapon	**Internal OR External exclusion** **Notify local authority** **Contact Police**	**5**	Head Teacher Head Teacher

Within our behaviour policy trained staff are allowed to use Team Teach as a form of restraint.

Playtime and lunchtime Rules and Consequences

Rules

- **Do** respect play leaders and adults
- **Do** be kind to others and be a good friend
- **Do** play games fairly and respect equipment
- **Do** keep safe
- **Do** be respectful and fair

Consequences

- **Stage 1- Yellow car**🟨 -- remind child of expected behaviour. Choice presented to child, " You can choose to……..or you can choose to break the rules then you will have time out.**"**
- **Stage 2- Yellow car**🟨 - Timeout in playground for 5 minutes- recorded in behaviour book. Choice presented to child
- **Stage 3- Red Card**🟥 - Timeout in Sycamore Suite for remainder of lunchtime. Recorded in behaviour book.
- **Continue to disobey rules**- sent to Sycamore Suite, Head teacher informed, and child may be excluded off the playground for a set period of time- parents notified.

Woodlands Academy of Learning

GDPR Data Protection Policy

CONTENTS

1 INTRODUCTION

1.1 Woodlands Academy of Learning collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory responsibilities.

1.2 School staff are obliged to comply with this Policy when processing Personal Data on the school's behalf. Any breach of this Policy by school staff may result in disciplinary or other action.

2 ABOUT THIS POLICY

2.1 The school holds Personal Data about current, past and prospective pupils, parents, employees and others with whom the school communicates. Personal Data may be recorded on paper, stored electronically, visual media or other formats.

2.2 This Policy and other documents referred to in it set out the basis on which the school will process any Personal Data it collects from individuals, whether those data are provided to us by individuals or obtained from other sources. It sets out the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.

2.3 This Policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 The Data Protection Officer is responsible for supporting the school with compliance with the Relevant Data Protection Laws and with this Policy. That post is held by Services4Schools Ltd. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer. The Data Protection Officer can be contacted at dpo@woodlands.walsall.sch.uk

3 DEFINITION OF DATA PROTECTION TERMS

3.1 In this Policy, the functions of the school are the provision of education and any pastoral, business, administrative, community or similar activities associated with that provision. References to the school 'carrying out its functions' or similar are references to these activities.

3.2 References to 'we' are references to the school.

3.3 Data Subjects means identified or identifiable natural (living) persons whose Personal Data the school holds. These may be pupils, parents/carers, staff, governors, visitors etc. This Policy also refers to Data Subjects as 'individuals.'

3.4 Data Controllers are the people who, or organisations which, determine the purposes for which any Personal Data are processed, including the means of the processing. The school is the Data Controller of all Personal Data used for carrying out its functions.

3.5 School Staff are, for the purposes of this Policy, those of our employees whose work involves processing Personal Data. School staff must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times.

3.6 Data Processors include any person or organisation, who is not a member of school staff, which processes Personal Data on the school's behalf, including any external suppliers that handle Personal Data on the school's behalf.

3.7 Privacy Notices are documents explaining to Data Subjects how their data will be used by the school.

3.8 Personal Data means any information relating to an identified or identifiable natural (living) person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.9 Personal Data Breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data the school is responsible for.

3.10 Pseudonymisation means the processing of Personal Data so that it can no longer be attributed to a specific person without the use of additional information. This additional information (or key) must be kept separately and is subject to measures to ensure that the identity of the Data Subject remains protected.

3.11 Relevant Data Protection Law means the Data Protection Act 2018, the General Data Protection Regulation ((EU) 2016/679), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) and all applicable laws and regulations relating to the processing of Personal Data and privacy as amended, re-enacted, replaced or superseded from time to time and where applicable the guidance and codes of practice issued by the United Kingdom's Information Commissioner.

3.12 Special Categories of Personal Data (formerly known as 'sensitive Personal Data') includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and genetic or biological traits. Special Categories of Personal Data can only be processed under strict conditions.

4 DATA PROTECTION PRINCIPLES

4.1 Anyone processing Personal Data for, or on behalf of, the school must comply with the principles of good practice contained in Relevant Data Protection Law. These principles state that Personal Data must be:

4.1.1 processed fairly, lawfully and transparently;

4.1.2 processed for specified, limited and legitimate purposes and in an appropriate way;

4.1.3 adequate, relevant and not excessive for the purposes for which they are processed;

4.1.4 accurate and, where necessary, kept up to date;

4.1.5 not kept longer than necessary for the intended purpose of processing; and

4.1.6 processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The school will keep a record of all Data Processing activities and must be able to demonstrate its compliance with these principles and with the wider requirements of Relevant Data Protection Law.

5 FAIR, LAWFUL AND TRANSPARENT PROCESSING

5.1 For Personal Data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in Relevant Data Protection Law. These include, but are not limited to:

5.1.1 the individual's explicit consent to the processing for one or more specified purposes;

5.1.2 that the processing is necessary for the performance of a contract with the individual or for the compliance with a legal obligation to which the school is subject;

5.1.3 that the processing is in the public interest; or

5.1.4 that the processing is in the legitimate interest of the school or relevant third parties to which the data are disclosed, so long as this is balanced with the rights and freedoms of the individual.

5.2 Where a change to a process, or introduction of a new process involving the use of large volumes of Data Processing, that is likely to pose a high risk to individuals' rights, the school will carry out an appropriate Privacy Impact Assessment.

5.3 Special Categories of Personal Data

5.4 When Special Categories of Personal Data are being processed, the individual's explicit consent to processing of those data must be obtained unless the processing:

5.4.1 is necessary for the purposes of carrying out the obligations and exercising specific rights of the school or of the individual in the field of employment and social security and social protection law;

5.4.2 is necessary for the assessment of the working capacity of an individual where the individual is an employee or for the provision of health or social care;

5.4.3 relates to Personal Data which are manifestly made public by the individual;

5.4.4 is necessary for reasons of substantial public interest; or

5.4.5 is necessary to protect the vital interests of the individual.

5.5 Processing of data relating to Criminal Convictions and Offences can only take place under control of an official authority, such as instructions from the police or an order of the court, or where UK or EU law states that processing must take place.

5.5.1 This is undertaken as part of the pre-employment check process (DBS) for all staff employed by the school, or where it is necessary to perform such a check as required by safeguarding regulation.

5.6 Consent of adults and organisations

5.7 Where an individual gives consent to Data Processing, that consent must be freely given, specific, informed and unambiguous and should be either in the form of a statement (whether or not prepared by the school) or a positive action demonstrating consent. Any requests that the school makes for consent must be in clear language.

5.8 An individual has the right to withdraw consent at any time and will be informed of this right and how to exercise it when the school requests consent.

5.9 Consent of children and young people

5.10 Parental consent to Data Processing must be obtained for pupils or other children younger than 16 years of age.

6 PROCESSING FOR SPECIFIED, LIMITED AND LEGITIMATE PURPOSES

6.1 In the course of carrying out its functions, the school may collect and process the Personal Data set out in its data asset register. This may include data we receive directly from an individual (for example, by completing forms or by corresponding with us by post, phone, email or otherwise) and data we receive from other sources (including, for example, parents/carers, other schools, the local authority or other public bodies, recruitment agencies or service providers, professional advisers and others).

6.2 The school will only process Personal Data for the specific purposes set out in

Information Asset Register or for any other purposes specifically permitted by Relevant Data Protection Law. We will explain those purposes to the Data Subject via Privacy Notices, or consent forms as appropriate.

7 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 We will only collect Personal Data to the extent that it is required for the specific purpose notified to the individual.

7.2 If a member of staff has any doubt as to whether any processing exceeds the purposes for which that data was originally collected, he or she should notify the Data Protection Officer.

8 ACCURATE AND UP-TO-DATE DATA

8.1 We will ensure that Personal Data we hold are accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

8.2 It is the responsibility of staff to ensure that Personal Data is accurate and kept up to date. All staff must as a minimum check that any Personal Data that they provide to the school in connection with their employment is accurate and up to date. They must also inform the school of any changes to their Personal Data that they have provided, e.g. change of address, either at the time of appointment or subsequently.

9 TIMELY PROCESSING

9.1 We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which are no longer required. We will be guided by the Information Records Management Society guidance in respect of decision making concerning the retention of Personal Data (Schools Toolkit 2016).

9.2 If a member of staff has any doubt as to whether any Personal Data has been or will be kept longer than is necessary for the purpose or purposes for which they were collected, he or she should notify the Data Protection Officer.

10 PROCESSING SECURELY AND IN LINE WITH RIGHTS OF DATA SUBJECTS

10.1 We are committed to upholding the rights of individuals to access Personal Data the school holds on them.

10.2 We will process all Personal Data in line with individuals' rights, in particular their rights to:

10.2.1 be informed, in a manner which is concise, transparent, intelligible and easily accessible and written in clear and plain language, of the purpose, use, recipients and other processing issues relating to data;

10.2.2 receive confirmation as to whether your Personal Data is being processed by us;

10.2.3 access your Personal Data which we are processing only by formal written request. We may charge you for exercising this right if we are allowed to do so by Relevant Data Protection Law. School employees who receive a written request should forward it to their line managers and the Data Protection Officer immediately;

10.2.4 have data amended or deleted under certain circumstances where data is inaccurate or to have data completed where data is incomplete by providing a supplementary statement to the school (see also Paragraph 8);

10.2.5 restrict processing of data if one of the following circumstances applies:

a) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the controller to verify the accuracy of the Personal Data;

b) the processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;

c) the controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;

d) the Data Subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the Data Subject.

10.2.6 Where processing has been restricted, as above, such Personal Data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest and the Data Subject shall be informed.

10.2.7 Where processing is restricted under one of the grounds in Paragraph 10.2.5, the data shall only be processed with the individual's consent or in relation to the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or the United Kingdom.

10.2.8 An individual who has obtained restriction of processing under Paragraph 10.2.5 shall be informed by the school before the restriction of processing is lifted.

10.2.9 Receive data concerning the individual, which he or she has provided to the school and is processed by automated means, in a structured, commonly used and machine-readable format and to transmit those data to another controller without hindrance from the school.

10.2.10 Object to Data Processing on grounds relating to his or her particular situation unless the school demonstrates compelling legitimate grounds for processing which overrides the interests, rights and freedoms of the individual or for to the establishment, exercise or defence of legal claims; and

10.2.11 Not to be subject to a decision based solely on automated decision-making and profiling which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is based on the individual's explicit consent.

10.3 It is the responsibility of all staff to ensure that any request by an individual under Paragraph 10.1 is brought to the attention of the Data Protection Officer without undue delay.

10.4 The school may refuse a request by an individual wishing to exercise one of the above rights in accordance with Relevant Data Protection Law.

10.5 The school shall provide information on action taken on a request under Paragraph 10.1 to the individual within one month of receipt of the request unless the school deems it necessary to extend this period by two further months where the request is complex and informs the individual of such extension with reasons within one month of receipt of the request.

10.6 If a request under Paragraph 10.2 is unfounded or excessive, the school may charge a reasonable fee for providing the information or refuse the request.

10.7 When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:

10.7.1 We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

10.7.2 We will suggest that the caller put his or her request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

10.8 Our employees will refer a request to the Headteacher and the Data Protection Officer. Employees should not be bullied into disclosing personal information.

11 NOTIFYING DATA SUBJECTS

11.1 If we collect Personal Data directly from individuals, we will at the time of collection inform them about the processing including:

11.1.1 the identity and contact details for the school and its Data Protection

Officer;

11.1.2 the purpose or purposes for which we intend to process those Personal Data;

11.1.3 the types of third parties, if any, with which we will share or to which we will disclose those Personal Data; and

11.1.4 the means, if any, by which individuals can limit our use and sharing of their Personal Data.

11.2 If we receive Personal Data from a source other than the individual we will, except in certain circumstances, provide the individual with the information in Paragraph 11.1 above at the following times:

11.2.1 within one month of receiving the Personal Data;

11.2.2 if the Personal Data are to be used for communication with the individual, at the time of the first communication to the individual;

11.2.3 if a disclosure to another recipient is envisaged by us, at the time of the disclosure to that recipient.

11.3 A notification in the form of a Privacy Notice will be in writing or via a link to our website, unless the individual requests an oral notification.

11.4 We will also inform individuals whose Personal Data we process that the school is the Data Controller with regard to those data and who the Data Protection Officer is.

12 DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

12.2 We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Data Processor if he or she agrees to comply with those procedures and policies, or if he or she puts in place adequate measures.

12.3 School staff will be issued with details of their obligations in relation to security of Personal Data.

12.4 All school staff must:

12.4.1 assist the school in upholding individuals' Data Protection rights;

12.4.2 only act in accordance with the school's instructions and authorisation;

12.4.3 notify the Data Protection Officer immediately of any Personal Data Breaches, allegations of Personal Data Breaches or suspicions of Personal Data Breaches in accordance with Paragraph 12.5;

12.4.4 comply at all times with the terms of any agreements with the school and with their responsibilities under Relevant Data Protection Law;

12.4.5 satisfy the school, within a reasonable period following request, of their compliance with the provisions of Paragraph 12.4.4.

12.5 The school will notify the Information Commissioner's Office of any Personal Data Breaches without undue delay.

12.6 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

12.6.1 Confidentiality: only people who are authorised to use the data can access them;

12.6.2 Integrity: Personal Data should be accurate and suitable for the purpose for which they are processed;

12.6.3 Availability: authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on the school's central computer system instead of on individual computers, tablets or other media.

12.7 Security procedures include:

12.7.1 IT Equipment: Staff must ensure they have read the school's ICT policy before using school equipment, individual monitors do not show confidential information to passers-by and that they log off from their computers, tablets or other devices when left unattended.

12.7.2 Building Security and Entry controls: All visitors are required to sign in using appropriate systems. Any unauthorised person seen on the school's premises should be reported.

12.7.3 Secure lockable storage: Rooms, desks, cupboards and filing cabinets should be kept locked when unattended if they hold confidential information of any kind (personal information is always considered confidential).

12.7.4 Appropriate Sharing and Verbal Disclosure: When providing personal information verbally, particularly by telephone, it is most important that the individual's identity is verified before any information is disclosed and that conversations occur in a space where information cannot be overheard.

12.7.5 Methods of disposal: Paper documents containing personal information should be shredded when they are no longer needed. Digital storage devices should be handed into relevant staff at the school to be securely destroyed when they are no longer required.

12.7.6 Personal Data on display: All Personal Data displayed in the school's buildings will be limited to what is necessary and pseudonymised where appropriate. If Personal Data is displayed externally, then consent should be sought prior to publication.

12.7.7 Electronic Transport/Transfer of Personal Data: School staff will use only approved methods to transport or transfer data as detailed in the school's ICT policy.

12.7.8 Photographs and Digital Images: (including video). We use photographs and digital images for a variety of purposes across the school, these include, but are not limited to:

- Capturing development and progress in learning
- School prospectuses and other publications focussed on promoting the school
- Assemblies and celebration events
- Sports day
- School performances
- Social Media
- Trips and residential outings

12.8 Where images of children or staff are used in public areas or made available online via publication on the school's website, the school will always seek consent before images are published.

12.9 The school shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement Data Protection principles and to integrate the necessary safeguards into processing activities.

12.10 The school shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed.

13 REGISTER OF PROCESSING ACTIVITIES

13.1 The school must maintain an accurate and up-to-date Information Asset Register of processing activities carried out by the school.

13.2 The school must record the following information for each processing activity:

13.2.1 the contact details for the school and its Data Protection Officer;

13.2.2 the purpose or purposes for which the processing activity has occurred;

13.2.3 descriptions of the categories of individuals involved in the processing activity;

13.2.4 descriptions of the categories of Personal Data involved in the processing activity;

13.2.5 descriptions of the categories of recipients of the Personal Data involved in the processing activity;

13.2.6 details of any transfers to third parties, including documentation of the transfer mechanism safeguards in place;

13.2.7 retention schedules;

13.2.8 descriptions of technical and organisational security measures in place relating to the processing activity.

13.3 It is the responsibility of all staff, to notify the Data Protection Officer of any changes that affect the use of Personal Data to ensure that the register of processing activities is accurate and kept up to date.

14 REGISTER OF BREACHES

14.1 The school must maintain an accurate and up-to-date register of all Personal Data Breaches.

14.2 If anyone becomes aware of a Data Protection breach they must inform the Data Protection Officer immediately. A plan for managing Data Breaches will be made available to all staff.

15 DATA PROTECTION OFFICER

15.1 The Data Protection Officer is responsible for supporting the school in compliance with Relevant Data Protection Law and with this Policy. The Data Protection Officer reports to the school's Headteacher and Management Committee, but fulfils their Data Protection functions independently.

15.2 The Data Protection Officer for the school is provided by Services4 Schools Ltd and can be contacted at dpo@woodlands.walsall.sch.uk or by writing to Woodlands Academy of Learning Bloxwich Road North, Short Heath, Willenhall, WV12 5PR. Please address letters: For the attention of the Data Protection Officer.

15.3 Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer.

15.4 Where a Personal Data Breach has occurred, it will be for the Data Protection Officer to decide whether, under the circumstances and in accordance with Relevant Data Protection Law, the individual concerned must be informed of the breach.

16 USING DATA PROCESSORS

16.1 The school retains the right to engage by written contract any person or organisation, who is not a member of school staff, to process Personal Data on our behalf.

16.2 Data Processors must:

16.2.1 assist the school in upholding individuals' Data Protection rights;

16.2.2 only act in accordance with the school's instructions and authorisation;

16.2.3 maintain a written record of processing activities carried out on behalf of the school and provide this to the school within [a reasonable period] following request;

16.2.4 notify the school of Personal Data Breaches without undue delay and maintain a register of breaches in accordance with Paragraph 13;

16.2.5 comply at all times with the terms of any agreements with the school and with their responsibilities under Relevant Data Protection Law;

16.2.6 satisfy the school, within a reasonable period following request, of their compliance with the provisions of Paragraph 12.4.4.

17 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

17.1 Individuals have particular rights with regard to transfers of their Personal Data outside the European Economic Area ('EEA'). Circumstances in which the school may need to transfer data outside the EEA might include use of IT services hosted overseas, arrangement and administration of school trips and cultural exchange projects.

17.2 Subject to the requirements in Paragraph 12.1 above, Personal Data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff may be engaged, among other things, in the processing of payment details and the provision of support services.

17.3 We may transfer any Personal Data we hold to a country outside the EEA provided that:

17.3.1 the transfer to the country or countries in question is permitted by Relevant Data Protection Law; and

17.3.2 any transfer to a country or countries outside the EEA is subject the escalation procedure under Paragraph 17.4.

17.4 Before a transfer of Personal Data is made outside the EEA, the following safeguards must be provided to ensure that the rights of Data Subjects and effective legal remedies for Data Subjects are available:

17.4.1 confirmation by implementing act by the European Commission of the adequacy of the level of protection afforded by the relevant third country;

17.4.2 standard Data Protection Paragraphs adopted by the European Commission in accordance with Relevant Data Protection Law must be included in relevant documentation;

17.4.3 ensuring explicit consent is given by the Data Subject to the proposed transfer after having been informed of the possible risks of such transfer;

17.4.4 confirmation that the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject;

17.4.5 confirmation that the transfer is necessary for important reasons of public interest;

17.4.6 the Data Protection Officer must authorise the transfer.

18 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

18.1 We may share Personal Data we hold with staff within the school.

18.2 We may also disclose Personal Data we hold to third parties:

18.2.1 if we are under a duty to disclose or share an individual's Personal Data in order to comply with any legal obligation;

18.2.2 in order to enforce or apply any contract with the individual or other agreements; or

18.2.3 to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of child welfare and fraud protection.

18.3 We may also share Personal Data we hold with selected third parties for the purposes set out in the school's Information Asset Register

19 REQUESTS FOR INFORMATION

19.1 Requests for information may take the following forms:

19.1.1 Requests for education records.

19.1.2 Freedom of information requests.

19.1.3 Subject access requests.

19.2 Where a person with parental responsibility requests information about a child's educational records, then advice should be sought from the Data Protection Officer.

19.3 If a person makes a request for information under the Freedom of Information Act, then the information should usually be provided unless there are some specific concerns about disclosing the information. Common concerns in the school context may be that information relates to other people, is confidential or legally privileged. If a freedom of information request is made and there are any concerns about disclosing information, then the Data Protection Officer should be contacted.

19.4 If a person makes a subject access request, then they are requesting the personal information that the school has about them. There are exemptions to disclosing some information but these are more limited as a person has a right to know what information is held on them. If a subject access request is made, then the Data Protection Officer should be contacted immediately.

20 CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time. This Policy will be published on the school's website.