

# **FOX WOOD SCHOOL**



## **Online Safety Policy June 2020**

Head Teacher Lucinda Duffy

Fox Wood School  
Holes Lane  
Warrington  
WA1 4LS  
Tel: 01925 811534

## **Introduction**

### **The use of the Internet at Fox Wood School is a privilege.**

Fox Wood School recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good online. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

Online safety covers the Internet, but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school safeguarding issue and responsibility.

## **1. Roles and Responsibilities**

**The school online safety coordinator is Gemma Greaves**

**The designated member of the governing body responsible for online safety is Trish Chapman (Chair of Governors and Safeguarding Governor)**

### **Governors**

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing online incidents and monitoring reports. Online safety falls within the remit of the governor responsible for Safeguarding. The role of the online safety governor will include:

- ensure an online safety policy is in place, reviewed every year and/or in response to an incident and is available to all stakeholders
- ensure that there is an online safety coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive
- ensure that procedures for the safe use of ICT and the Internet are in place and adhered to
- hold the headteacher and staff accountable for online safety.
- Online safety will be discussed at half termly Safeguarding meetings held between the named governor and the Designated Safeguarding Lead (DSL)

### **Headteacher and SLT**

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety co-ordinator. Any complaint about staff misuse must be referred to the online safety coordinator at the school or, in the case of a serious complaint, to the headteacher.

- Ensure access to induction and training in online safety practices for all users.
- Ensure all staff receive regular, up to date training.
- Ensure appropriate action is taken in all cases of misuse.

- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SLT.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured.
- Work in partnership with the DfE, the Internet Service Provider and school ICT Manager to ensure systems to protect students are appropriate and managed correctly.
- Ensure the school ICT system is reviewed regularly regarding security and that virus protection is installed and updated regularly.
- The Senior Leadership Team will receive monitoring reports from the online safety co-ordinator.

**Online safety coordinator:**

- Leads online safety meetings/training sessions.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Reports to Senior Leadership Team.

**ICT Support Company – UTL:**

UTL are responsible for ensuring:

- That the schools technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / Internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the headteacher; online safety coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.

## **2. Communicating School Policy**

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school Code of Conduct when online, and online safety guidelines, are displayed around the school. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

## **3. Making use of ICT and the Internet in school**

Fox Wood school encourages the use of Computing (including Computer Science, Information Technology and Digital Literacy) in a responsible way, in order to enhance pupils' experience and raise standards. Staff and Governors have access to the School's Computing system to support these aims, (including Internet and Email), subject to a written undertaking to abide by this Code of Conduct. Pupils have access to Internet and Email facilities with staff support. The Governing Body recognises that the development of staff expertise relies on frequent use of these technologies. Therefore, subject to considerations of cost and considerations of "abuse" staff are permitted to use the School's Computing facilities for professional use and personal use when agreed with a member of the Senior Leadership Team (SLT). (This permission may be withdrawn without alteration to this document, if circumstances change.) All staff should be aware that the school Computing equipment has security monitoring

software called Securus. The use of mobile phones when working with pupils is also prohibited, unless agreed to by the SLT on a very rare occasion if the need arises.

Some of the benefits of using ICT and the Internet in schools are:

**For pupils:**

- Opportunities to develop their ideas and interests
- Unlimited access to worldwide educational resources
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to videos and interactive media to enhance understanding.
- Individualised access to learning.
- Opportunities to develop their independence

**For staff:**

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

## **4. Learning to Evaluate Internet Content**

With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiarism very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. When using a network workstation all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators (UTL) can manually add site addresses which are considered to be unacceptable. However, no system is 100% safe and we expect users to behave responsibly. To underpin this we have a security monitoring program called "Securus". Users are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly and that some sites can damage your computers. We monitor all access to websites that may be unsuitable for children and/or containing offensive language, images, games or other media. If staff or pupils discover unsuitable sites, then the URL will be reported to the *school online safety coordinator*. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities; any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took

place at school. We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the Internet. We do not allow staff to “friend” parents or pupils on social media sites. If they are approached they must inform the school SLT immediately.

### **Pupil use of the Internet.**

Pupils shall be able to use the Internet under the following conditions:

- The Code of Conduct will be adhered to by all pupils who use the Internet within the school
- The Internet is provided for the education of and the improved delivery of curriculum material(s). Pupils are encouraged to make use of the services to this end.
- All pupils are supervised as they use the Internet, a staff member is always in the room. We also have Securus our monitoring software, on all machines which alerts SLT to possible misuse.

**Our pupils at Fox Wood have a range of Special Educational Needs and require additional support to safeguard themselves.**

- Some pupils may need additional teaching that includes reminders and explicit prompts of how to keep safe when using the Internet.
- Visual support is important to aid pupils’ understanding and pupils may respond well to multi-media presentations of Online Safety rules, such as interactive PowerPoint slides, sounds and recordings.
- Many of our pupils have limited social understanding which may leave them open to risks when using the Internet individually and also when with peers. Adults need to plan group interactions carefully when raising awareness of Internet safety.
- Some of our pupils choose recreational Internet activities that may be aimed at pupils younger than themselves. By their very nature, these activities tend to be more controlled and less open to naïve mistakes. Staff need to plan how to manage pupils who may want to do the same as other peers but who may need small step teaching due to limited experiences with Internet use.

## **5. Managing Information Systems and Computing Provision**

The school is responsible for reviewing and managing the security of the computers and Internet networks and takes the protection of school data and personal protection of our school community very seriously.

### **Physical Safety**

- All electrical equipment in the school is subject to “PAT” testing (Portable Appliance Testing) and is tested regularly to ensure that it is safe to use.
- Workstations are cleaned and sanitised regularly. Pupils are taught to avoid taking food and liquids anywhere near the computers. We expect all users to refrain from eating and drinking when working at a computer
- Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. Comfort of pupils is taken into account when setting heights of rise and fall tables and peripherals required by our pupils with PMLD. We expect all users to take responsibility for their own physical well-being by adopting good practices.
- Computers and other Computing equipment can be easily damaged. We expect staff and pupils to respect Computing equipment by taking care when handling and using.
- Staff must also ensure they report any damage.

### **Network Safety**

All users have an individual log on using a username and password.

- More-able pupils have a full username and password which they are encouraged to change regularly.
- Less able pupils log on using only initials. (pupils may require 1-1 Physical/verbal support to do this.)
- All staff have their own log-ons and are reminded to not share or write it down.
- We expect all users to only logon using their username.
- Staff are asked to lock their workstation when they are not working on it to maintain their own security.
- The above is monitored by spot visits by the SLT and Securus Monitoring Software and reported back to the Computing team and the relevant staff

## Monitoring Software

### ***The school has monitoring software on all Computers and Laptops (Securus).***

Securus Education detects inappropriate content as soon as it appears on screen, whether it has been typed or received by the user. A screen capture is taken of every incident, showing what was displayed at the time, who was involved and when the incident took place. This software was designed by the police and records all use of computers and cannot be removed once installed. Laptops also have this software and when they attach to the school network any Securus logs are automatically uploaded to the Securus server. The system creates security logs which if a threshold is met sends an email to the appropriate member of SLT. Securus is monitored by the Deputy Headteacher and Office Manager.

- All staff and users or appropriate adults (for students) are aware of the Securus program and have signed the Computing Code of Conduct.
- Each user is given a "Home drive" (My documents). Where appropriate pupils are taught how to save their work into their "Home drive" area. We help and support pupils to save and keep their work to build up a portfolio of evidence.
- Access to other users "Home drive" areas are restricted by the network. Users are taught not to access another user's work without permission. We expect users to respect the privacy of all other users and to make no attempt to access or interfere with another user's work.
- On the network there are "shared resource" areas where many different groups of users can save work so that it is available to others. Users are taught how to access and save to these shared resource areas. We expect users to respect the contributions of others, not to delete or alter others' work and to ensure that they only save work to shared areas with permission. Confidential data or data we do not wish to be edited is 'read only'.
- Printing is not at the moment restricted but can be monitored. Staff have to use their username to access their documents from the printer. Logs are kept of the documents printed by each username. The default print setting is black and white. Users are taught to only print when necessary to save resources for financial and environmental reasons.
- The network software prevents changes being made to computer settings. Users are taught that making changes may prevent the computer from working properly.
- Only the network administrators are permitted to install software on to computers.
- All users of the network can be monitored remotely by the network administrators. We expect all users to understand that their use is subject to monitoring.

## 6. Emails

The school uses email internally for staff and pupils to make contact with other pupils, staff or establishments. Pupil's accessing their emails should always be supervised by a member of staff. Email accounts are set up for the intended user only. Unauthorised use of other people's accounts to send and receive emails is unacceptable. We expect all users to communicate in an appropriate manner through email. Staff and pupils should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

Some pupils will have their own webmail accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. Therefore, we do not permit the use of personalised email accounts by pupils at school or at home for school purposes. Pupils are taught that using a personalised webmail account in school or for school use is not permitted. We expect pupils to use school issued email accounts only whilst in school.

Whilst staff are allowed to access their own home/personal email accounts in school, they are aware that all access is monitored by "Securus", also that it is limited to break times or before or after work.

## 7. Published Content and the School Website

The school website address is **[www.foxwoodschool.org.uk](http://www.foxwoodschool.org.uk)**

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. The website also contains statutory documents and other important school documents such as policies and procedures. Photographs are only displayed with parental permission and pupil's names will not appear in full. We expect all persons accessing the school website to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office or for individuals who have agreed to sharing email address. All teachers, SLT and admin staff have access to edit the website. Any staff editing the website need to ensure that what they are uploading is appropriate and in line with policy guidelines. The website is monitored by the Computing lead and SLT. **For information on the school policy on children's photographs on the school website please refer to section 7.1 of this policy.**

## 7.1 Guidance of Safe Use of Children's Photographs and Work

Colour photographs and pupils work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the General Data Protection Regulation 2018 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. For students 13 and above their explicit consent is also required. The school does this to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period rather than a one-off incident does not affect what you are consenting to. **Parents will be contacted annually for consent.**

## 7.2 Using photographs of individual children

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children.

- Parents and others attending school events can take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The school does not prohibit this as a matter of policy.
- The school does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the school to prevent.
- Fox Wood School asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.
- As a school we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.
- Whenever a pupil begins their attendance at Fox Wood School they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.
- Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **complaints policy** for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the school's **child protection and safeguarding policy** and **behaviour policy**.
- Misuse of photographs or videos in any form will be dealt with in accordance with the school Behaviour Policy according to the incident type.

### 7.3 Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are potentially more vulnerable to content, contact and conduct behavioural issues. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the Computing curriculum and PSHEE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's Code of Conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or student's/class groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are always representing the school and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

## 8. Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make pupils and staff more vulnerable to cyberbullying
- Can be used to access inappropriate Internet material
- Can be a distraction in the classroom
- Are valuable items that could be stolen, damaged, or lost
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined below.

- Mobile phones should not be used within the school building with the exception of in the staff room during staff breaks and in classrooms after all pupils have left the school grounds.
- The school will not tolerate cyber bullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the **school behaviour policy**.
- If staff wish to use these devices in class as part of a learning project, they must get permission from a member of the senior leadership team.

### 8.1 Mobile Phone or Personal Device Misuse

- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours and kept away from pupils.

- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the **child protection and safeguarding policy**, or in the staff contract of employment.

## 9. Cyberbullying

The school, as with any other form of bullying, takes Cyber bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the **behaviour policy and the school anti-bullying guidance**. The anonymity that can come with using the Internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it.

## 10. Cyberbullying

Extending Computing experiences at home is both valued and encouraged. Parents/carers will be asked for their permission for our pupils to use the Internet and comply with our conditions of use. Parents have been invited to attend Family Learning sessions in school including Computing training. Parents are offered the chance to discuss appropriate Computing equipment used by their son/daughter in school e.g. access devices, and can attend sessions where they are shown how to use these and where to obtain such items should they be interested.

## 11. Conditions of Use

The Internet is available to staff, pupils and governors and other invited persons under the following conditions.

A copy of these conditions is distributed to all users and parents/carers, they sign and acknowledge acceptance of the conditions. A copy of these conditions will also be available in every class and in the staff room.

### Staff

- All members of staff are responsible for explaining the rules and implications of possible misuses of the Internet and their responsibilities towards the pupils.
- Staff using the Internet in school will be required to sign a copy of the "Code of Conduct".
- Fox Wood school staff are required to connect their staff laptops to the school network at least once a week during term time to ensure antivirus and updates are carried out

All staff whether part time, full time, teaching staff or non-teaching staff are allowed access to the Internet in accordance with the following provisions.

All Internet use shall be for the purpose of:

- Looking for information so that pupils or staff may gain a better understanding of a subject.
- For staff training purposes where the information is available via the Internet.
- The use of e-mail for contact with other businesses or establishments on school business or to request information for the benefit of the school.

The Internet should be used in a professional manner. Internet use using the World Wide Web (WWW) and Internet phone and fax services shall be for school purposes only unless with consent of the head teacher.

All staff members receive training on how to access the school website.

## **Pupils**

Pupils shall be able to use the Internet under the following conditions:

- The Code of Conduct will be adhered to by all pupils who use the Internet within the school
- The Internet is provided for the education of and the improved delivery of curriculum material(s). Pupils are encouraged to make use of the services to this end.
- All pupils are supervised as they use the Internet, a staff member is always in the room. We also have Securus our monitoring software, on all machines which alerts SLT to possible misuse.

## **Use of service**

- No profanity or obscenities are to be used in any e-mail messages. We use RM Easymail and this does restrict swearing etc and an email is sent to the webmaster if rules are violated. This is then passed to the schools SLT.
- No private information is to be distributed to other parties at any time. This includes reposting of information sent by another party.
- The network is not to be used by any member of staff or pupils for personal gain or illegal activity.
- Deliberate attempts to gain access to WWW containing material of pornographic, racially or religiously offensive or illegal material will be dealt with as a serious breach of school rules.
- Downloading of material must be scanned for viruses at all times and any deliberate attempt to spread viruses through the network will be seen as a breach of the guidelines and dealt with as such.
- All copyright, privacy and international laws are to be abided by at all times.

## **12. Liability**

Fox Wood School is not, and cannot be held responsible for the loss of material, accidental corruption or any other action that might affect transmission or loss of data.

Fox Wood School has taken all possible precautions to maintain the safety of all users and these guidelines are written and enforced in the interest of all users' safety and effective use of the Internet. The Local Authority via the Warrington Wide Area Network filters all Internet access into the school. Fox Wood also has an additional firewall for further protection. During school all staff will guide our pupils towards the appropriate materials. Staff will not knowingly set pupils homework where the topics of research would lead to unsavoury sites and staff will visit suggested websites for viability before any lesson is undertaken.

Outside of school, families have responsibility for guiding their child's use of the Internet, although Fox Wood communicates with parents and carers to reinforce safe procedures at home. It is school's responsibility to give pupils a basic understanding of Online Safety

## **13. Protecting Personal Data**

Fox Wood School believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect, and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the General Data Protection Regulation 2018, and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection **read the school's data protection policy.**

#### **14. Abuse of guidelines**

Those staff who abuse these guidelines will be dealt with accordingly. Please see the "Code of Conduct"

**In all cases of abuse the police and/or the local authorities may be involved.**

#### **15. Summary**

We have in place the above management systems to protect the interests of management, staff, pupils and parents. The policy will be reviewed regularly.