Windy Arbor Primary School
E-SAFETY POLICY

Based on
Solihull Schools' e-Safety Policy

Policy written/reviewed by:	A Theay/J Stinson
Date:	September 2023
Ratified by Governors on:	
Signed:	
Date to be reviewed:	September 2025

This document owes much to the work of both Kent and Warwickshire in relation to e-safety. Their thinking and documentation has been a great support to the development of the e-safety policy in Solihull

Solihull Metropolitan Borough Council

Contents

1. Who writes and reviews the policy? Page 3
2. Why Internet use is important Page 3
3. Benefits of the Internet to education Page 4
4. How the Internet enhances learning Page 4
    - 4.1 Pupils Page 5
    - 4.2 Staff Page 6
    - 4.3 Parents Page 6
5. Internet access Page 7
6. Pupils evaluating Internet content Page 8
7. Managing published content Page 8
8. Publishing images of staff and pupils Page 9
9. Managing social networking Page 10
10. Managing filtering Page 11
11. Managing email Page 12
12. Video conferencing Page 13
13. Emerging technologies Page 14
14. Managing Information Services Page 15
15. Protecting personal data Page 16
16. E-Safety complaints Page 17

1. Who writes and reviews the policy?	The e-Safety Policy provides an important part of schools' safeguarding provision for pupils. It is part of the Computing Policy and School Development Plan and should relate to other policies including those for behaviour, personal, social and health education (PSHE) and for citizenship. Writing the policy provides an opportunity to review practice, in this case the use of a major technology and its benefits and risks. The more that staff, parents, governors and pupils are involved in deciding the policy, the more effective it will be.	*The school's e-Safety Coordinator is Mr. A. Theay, who will be responsible for writing and reviewing this policy with Mr.J.Stinson. Mr A.Theay is responsible for the Computing curriculum in school and Mr J.Stinson is responsible for maintaining the schools network infrastructure, social media and website..*
		Our e-Safety Policy has been written by the school, building on the SMBC Schools' e-Safety Policy and government guidance, as well as the school's experience. It has been agreed by the senior management and approved by governors.
		The e-Safety Policy and its implementation will be reviewed regularly (next review September 2025; 24 months' time).

2. Why Internet use is important	The rapid developments in electronic communications are having many effects, some profound, on society. Only a few years ago we were asking whether the Internet should be used in all schools. Now every pupil is younger than the World Wide Web and many use it more than their teachers. Nevertheless it is important to state what we are trying to achieve in education through use of the Internet and Information & Communication Technology.	The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
		Internet use is part of the statutory curriculum and a necessary tool for learning.
		Internet access is an entitlement for students who show a responsible and mature approach to its use.
		The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality and safe Internet access as part of their learning experience.
		Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

3. Benefits of the Internet to education	All Solihull schools have access to Broadband Internet connections. A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet. These benefits are outlined in the policy statements opposite.	Benefits of using the Internet in education include: • access to world-wide educational resources including museums and art galleries and to experts in many fields for pupils and staff; • inclusion in the National Education Network connecting all UK schools; • educational and cultural exchanges between pupils world-wide; • vocational, social and leisure use in libraries, clubs and at home; • professional development for staff through access to national developments, educational materials and effective curriculum practice; • collaboration across support services and professional associations; • improved access to technical support including remote management of networks and automatic system updates; • exchange of curriculum and administration data with SMBC and DCFS; • access to learning wherever and whenever convenient.

4. How the Internet enhances Learning	Increased computer numbers or improved Internet access may be provided but learning outcomes must also be addressed. Developing effective practice in Internet use for teaching and learning is essential. Librarians and teachers can help pupils to learn how to distil the meaning from the mass of information provided by the Internet. Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites, or teach search skills. Offering younger pupils a few good sites is often more effective than an Internet search. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.	*The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.*
		Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.
		Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
		Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
		Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

<table>
<tr>
<td rowspan="4">4.1 Pupils</td>
<td rowspan="4">Many pupils are very familiar with Internet use and culture and it might be wise to discuss and/or design elements of the School e-Safety Policy with them, possibly through a student council. As pupils' perceptions of the risks will vary, the rules for responsible use may need explanation and discussion. Pupils may need to be reminded of the school rules, possibly by posters at the point of Internet use.

Useful e-safety programmes include:

• Resources available via the WMNet website (www.wmnet.org.uk)
• Think U Know; currently available for primary and secondary pupils from (www.thinkuknow.co.uk)
• Internet Proficiency Scheme www.gridclub.com
• BBC Newsround Stay Safe Online http://www.bbc.co.uk/newsround/13910067</td>
<td>Rules for Internet access, as well as e-Safety guidance ('SMART',) will be posted around the school (one in every phase corridor).</td>
</tr>
<tr>
<td>Pupils will be informed that Internet use will be monitored. Both pupils and parents/carers will be made aware of and asked to read the acceptable use policy's relating to internet access before the pupil has there first ICT lesson, these polices are available on the school website.</td>
</tr>
<tr>
<td>An e-Safety training programme will be delivered to all pupils to raise the awareness and importance of safe and responsible use of the Internet and other electronic communications tools.*</td>
</tr>
<tr>
<td>Instruction in responsible and safe use should precede Internet access and will be reinforced at regular intervals (at the minimum, every academic year).

A module on responsible Internet use and e-Safety will be included in Computing lessons, covering both school and home use.

* The school will hold an 'E-Safety Week' to raise the profile of responsible Internet use and e-Safety amongst pupils, staff and parents.</td>
</tr>
</table>

4.2 Staff	It is important that all staff feel confident to use the Internet in teaching. The School e-Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation. Staff must understand that the Internet misuse rules for SMBC employees are quite specific. Instances of misuse resulting in dismissal have occurred. If a member of staff is concerned about any aspect of their Internet use in school, they should discuss this with their line manager to avoid any possible misunderstanding. Internet use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. The induction of new staff should discuss Internet issues, for instance the selection of appropriate modes of expression in email communication to prevent confusion.	*All staff will be given the School e-Safety Policy and its importance will be explained.* *Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff should be made aware of and have read the Internet usage policy as part of their induction to clearly outline what is permitted on the school network.* *Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.* *Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.*
4.3 Parents	Internet use in pupils' homes is now very widespread. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate, supervised use of the Internet at home. Parents should also be advised to check if pupils' use elsewhere (e.g. social networking) is covered by an appropriate use policy.	*Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school website and the school's Twitter feed.* *Internet issues will be handled sensitively to inform parents without alarm.* *A partnership approach with parents will be encouraged. This could include parents' sessions on e-Safety, but will at the minimum include informative material and guidance on e-Safety being sent home.* *Parents who are interested in learning more about safer Internet use can be referred to the guidance and links on the school website.*

5. Internet access	The school should allocate Internet access for staff and pupils on the basis of educational need, and in general access to the Internet will be universal for classroom professionals and for pupils. It should be clear who has Internet access and who has not. Authorisation is on an individual basis in all Solihull schools. In a primary school, where pupil usage is fully supervised, all pupils in a class could be authorised as a group. Parental permission will be required in all cases. As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system. Disclaimer for use: *In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SMBC can accept liability for the material accessed, or any consequences of Internet access.*	*The school will maintain a current record of all staff and pupils who are granted Internet access.* *All users must read, sign and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource.* *At Key Stage 1, access to the Internet will be by directly supervised access to specific, approved on-line materials.* *Parents will be informed that pupils will be provided with supervised Internet access (via a letter).* *Older primary children (KS2) must agree to comply with the Responsible Internet Use statement before they are granted access.* *Parents will be asked to sign and return a consent form for pupil access.* *The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.* *Methods to identify, assess and minimise risks will be reviewed regularly.* *The head teacher and e-Safety coordinator will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.*

6. Pupils evaluating Internet content	Information received via the Internet, email or text message requires good information handling skills. It may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. A whole curriculum approach to evaluating information may be required. Pupils should be taught research techniques and key information handling skills Pupils may occasionally be confronted with inappropriate material, despite filtering. They should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. Access to sensitive sites, for example those that record the Holocaust, may be required for the duration of a specific educational activity by supervised pupils of appropriate age. Pupils need to understand how to extract, interpret and use information and evaluate its significance. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.	*The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.* *If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to UNITY and Solihull ICT Services, and where appropriate the school e-Safety officer.* *Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy (Y5-6).* *Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work (all ages if/when appropriate).* *The evaluation (usefulness) of on-line materials is a part of every subject (all ages).*

7. Managing published content	A school's website can celebrate pupils' work, promote the school and publish resources for projects or homework. The website will reflect the school's ethos, ensure that information is accurate and up to date, and will be well presented. Personal security will be protected on the website. A school's website can be accessed by anyone. Publication of information should be considered from a security viewpoint. Material such as staff details or a detailed plan of the school may be better published in the school handbook and thereby be restricted to known persons.	*The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.* *Email addresses should be published carefully, to avoid spam harvesting.* *The Head Teacher and Website Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.* *The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.*

8. Publishing images of staff and pupils	Photographs that include pupils and/or staff add a liveliness and interest to a website. Nevertheless the security of staff and pupils must come first. Pupils' full names will never be published with their photographs. A check will be made that pupils in photographs are appropriately clothed. Photographs of a pupil should not be published without the parent's or carer's written permission. The school will ask for permission to publish images of work or appropriately taken photographs of pupils on entry to the school. Similarly, photographs of school staff should not be published without consent. Pupils need to be taught the reasons for caution in publishing personal information and photographs in social publishing sites.	*Photographs on the website and Twitter which include pupils will be selected carefully and will not enable individual pupils to be clearly identified (i.e. by name)* *Pupils' full names will not be used anywhere on the website or on Twitter, particularly in association with photographs.* *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or Twitter.* *Pupils' work will only be published with the permission of the pupil.* *Images of staff will not be published without consent.*

9. Managing social networking	Social networking sites can connect people with others for a wide range of purposes, including educational purposes. Guests can be invited to view personal space, pupils' work or documents and leave comments. There is increasing educational use of such tools, for example in the use of blogs and wikis to improve writing. Social networking has many possibilities for staff and pupils working together and is increasingly used in an educational context. A significant proportion of pupils in the upper years of KS2 and in secondary schools now use social networking out of school hours on a regular basis. They may need guidance and support in knowing how to stay safe on such sites and parents may not know what advice to give them. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published. Social networking sites can be used to bully others. Schools should ensure that pupils know what to do if they are bullied using social networking sites. Although most social networking sites are used outside school, the school has a responsibility along with parents to ensure that incidents of bullying are resolved. The use of communications tools is blurring the boundaries between home and school, both in learning and in the use of social networking. Schools have a responsibility to deal with incidents that take place after school if they involve school networks. They also have some responsibility to work with parents to prevent and to resolve with incidents that involve mobile phones or other social networking sites.	*Social networking sites and newsgroups (except Twitter which the school uses to share information) will be blocked unless a specific use is approved.* *Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.* *Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.* *Teachers should not run social network spaces for students on a personal basis. Teachers should not communicate with pupils through private social networking sites, even on educational matters, but should use official sites sanctioned by the school.* *Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students will be encouraged to invite known friends only and deny access to others. They will be advised not to publish specific and detailed private thoughts.* *We are aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments. Incidents of bullying through social networking will be dealt with in line with the school policy on bullying.*

10. Managing filtering	Levels of access and supervision should vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community and systems should be in place to adapt the access level according to pupils' specific areas of study are available and to meet staff needs. The technical strategies to restrict access to inappropriate material, fall into several overlapping types (commonly described as filtering): 1. Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day. 2. A 'walled-garden' or 'allow list' provides access only to a list of approved sites. Such lists inevitably restrict pupils' access to a narrow range of information. 3. Rating systems give each Web page a rating for sexual, profane, violent or other unacceptable content. There is a default level set on the web browser. 4. Access monitoring records the Internet sites visited by individual users. Access to a site forbidden by the filtering policy will result in a report. Solihull Council uses method (1) for filtering where it supplies an internet filtration service. Schools can opt to be responsible for their own filtering but, in these cases, need to be fully aware of what this involves. Taking responsibility for filtering can be only done with the agreement of Solihull Council and will only be approved where reassurances are given by the school as to the fitness of their systems.	*The school will work in partnership with Solihull MBC and Becta, as well as the UNITY ICT Network of which it is part, to ensure filtering systems are as effective as possible.* *If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school Network Manager or E-Safety coordinator.* *The Head Teacher, e-Safety Coordinator, School Network Manager and UNITY ICT Network manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.* *Any material that the school believes is illegal will be reported to appropriate agencies such as the Police, IWF or CEOP.*

11. Managing email	Email use can bring significant educational benefits and interesting projects between neighboring villages or towns, and even continents, can be created. However, un-regulated email can provide routes to pupils that bypass the traditional school boundaries and spam, phishing and virus attachment can make email risky. As with social networking, email can be used to bully others and the school has a responsibility, along with parents, to ensure that incidents of bullying are resolved. In the school context, email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and the preservation of privacy, both of which are covered by legislation. A central question is the degree of responsibility that can be delegated to individual pupils. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content and viruses is now possible. Schools should consider banning access to external web-based email, particularly as anonymous identities such as pjb354@mailhost.com make monitoring difficult. Strategies include limiting pupils to email accounts on the school domain or restricting email traffic to the school domain. Much email use is purely of a social nature. Is social email use considered to be useful experience of a communications tool or is it judged as low priority? Should access to social email only be made available outside lesson hours?	*Pupils may only use approved email accounts on the school system.* *Pupils must immediately tell a teacher if they receive offensive email.* *Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.* *Use of words included in the filtering/checking 'banned' list will be detected and logged.* *Whole-class or group email addresses could be used in primary schools and email will be supervised in a manner appropriate to the age of pupils concerned.* *Access in school (for pupils) to external personal email accounts will be blocked.* *Excessive social email use can interfere with learning and may be restricted.* *Email sent to external organisations will be written with due professional care.* *The forwarding of chain letters is not permitted.* *Email addresses will be published carefully, to avoid spam harvesting.* *Staff should only use email to communicate socially outside of lesson hours. Where there is an urgent need (e.g. in the case of sick relatives or legal matters), permission will have been sought from the Head Teacher in advance (as is the case with mobile phone usage).*

12. Video Conferencing (including Internet telephony such as Skype)	Video conferencing enables users to see and hear each other between different locations. It is a 'real time' interactive technology and has many uses in education. Equipment ranges from small PC systems (web cameras) to large room based systems that can be used for whole classes or lectures. The video conferencing equipment uses a 'network' to communicate with the other site. Video conferencing introduces new dimensions. Web cameras can enable limited video to be exchanged across the Internet. The availability of live video can increase safety – you can see who you are talking to – but if inappropriately used, a video link could reveal security details. Schools with full 'DCFS Specification' broadband are connected through the LA and Regional Broadband Consortia and have access to services such as gatekeepers and gateways to enable schools to communicate with other locations outside their LA. MCUs (Multipoint Control Units) enable several schools to communicate at one time, for instance with several video streams each in a screen window.	**The equipment and network** *All video conferencing equipment (including visualizer web cameras) in the classroom must be switched off when not in use and not set to auto answer.* *IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.* *Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.* *External IP addresses should not be made available to other sites.* *Video conferencing contact information should not be put on the school website* ***The school has begun to use Microsoft Teams to conduct video conferencing between staff other educational professional and outside agencies when required.*** **Users** *Pupils must ask permission from the supervising teacher before making or answering a video conference call.* *Video conferencing should be supervised appropriately for the pupils' age.* ***Any video calls within school are required to take place away from classrooms and pupil areas to respect pupil privacy and assure the safety of the pupils.*** **Content** *When recording a lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of video conference should be clear to all parties at the start of the conference.* *Recorded material shall be stored securely* *If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).* ***All participants of a virtual meeting will be made aware and asked to consent by the meeting host before any recording is started, they will also be made aware when the recording has ended. Recorded meeting will be stored securely on the network in a secured folder which only the appropriate staff (as decided by the Head Teacher) will have access to.***

13. Emerging technologies	Many emerging communications technologies offer the potential to develop new teaching and learning tools. A risk assessment needs to be undertaken on each new technology, and effective practice in classroom use should be developed. The safest approach is to deny or severely control and restrict access until a risk assessment has been completed and safety demonstrated. Virtual classrooms and virtual communities widen the geographical boundaries of learning. New requirements for online reporting to parents are being introduced. On-line communities may encourage a disaffected pupil to keep in touch or provide access to learning for an isolated pupil. The safety and effectiveness of wider virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites. The registering of individuals to establish and maintain validated electronic identities is an important part of the process. New applications are continually being developed based on the Internet, the mobile phone network, wireless or infrared connections. Wireless access has increased the mobility and range of access. This has led to a number of issues such as the videoing of teachers and the publication of the videos on social networking sites. Schools will need to consider appropriate responses to this type of behaviour. Schools should keep up to date with new technologies and communication methods and be ready to develop appropriate strategies. For instance text messaging is a frequent activity for many pupils that could be used for both appropriate and inappropriate activity in schools. The inclusion of inappropriate language or graphical icons within text messages is difficult for staff to detect. Pupils may need reminding that such usage is both inappropriate and conflicts with school policy. Abusive text messages would be dealt with under the school bullying policy.	*Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.* *The school's Mobile Devices Policy should be consulted for guidance on acceptable use of mobile phones and devices by pupils and staff in the school building and on school grounds.*

14. Managing Information Services	Information management is a complex and multi-faceted set of processes and cannot be dealt with adequately in this document. This is a major responsibility that includes delivery of essential services and has implications for the personal safety of staff and pupils. Effective information management requires a combination of robust technical systems and appropriate behaviour by the user. The most sophisticated information security system can be completely undermined by the member of staff who leaves the system logged on and unattended whilst they are distracted by something. A number of agencies can advise on security including Becta and Solihull's Information Strategy Manager. Local Area Network security issues include: • Users must act reasonably – the downloading of large files during the working day will affect the service that others receive. • Users must take responsibility for network use. For SMBC staff, disregarding ICT usage policy is regarded as a matter for dismissal. • Workstations should be secure from deliberate or opportunistic access by unauthorised users. • Servers must be located securely and physical access restricted. • The server operating system must be secure and kept up to date. • Virus protection for the whole network must be installed and current. • Access by wireless devices must be pro-actively managed and conform to technical standards recommended by Becta. • All Internet connections through Solihull Broadband will ensure compliance with the security policy. • Solihull Broadband firewalls and switches are configured to prevent unauthorised access between schools. • Decisions on WAN security are made on a partnership basis between school and Solihull Broadband.	*The security of the school information systems will be reviewed regularly.* *Virus protection will be updated regularly.* *Security strategies will follow Solihull MBC guidelines.* *Personal data sent over the Internet will be encrypted or otherwise secured.* *Portable media may not be used without specific permission followed by a virus check. Where they are used to store personal information they will be encrypted via BitLocker using AES 128 encryption (all staff will be encouraged to use Microsoft OneDrive as a secure alternative to portable media).* *Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.* *Files held on the school's network will be regularly checked.* *The UNITY ICT Network manager & School Network manager will review system capacity regularly.*

15. Protecting personal data	The quantity and variety of data held on pupils, families and on staff is expanding quite quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify an individual). The eight principles are that personal data must be: 1. Processed fairly and lawfully 2. Processed for specified purposes 3. Adequate, relevant and not excessive 4. Accurate and up-to-date 5. Held no longer than is necessary 6. Processed in line with individuals rights 7. Kept secure 8. Transferred only to other countries with suitable security measures.	*Personal data will be recorded, processed, transferred and made available in compliance with to the Data Protection Act 1998.* *Encryption will be provided for staff laptops wherever possible and all teaching staff will be encouraged to use Microsoft OneDrive to ensure data protection and security. Staff will be encouraged to save all sensitive school data (e.g. referring to pupils) on network drives to ensure data protection and security.*

16. e-safety complaints	Parents, teachers and pupils should know how to submit a complaint. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. A minor transgression of the rules by pupils may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's disciplinary policy. Complaints linked to staff should be dealt with by a senior member of staff. It is likely that most e-safety complaints will be dealt with using the normal complaints processes for the school. Potential child protection or illegal issues, however, must be referred to the school Designated Child Protection coordinator or e-Safety coordinator.	*Formal complaints of Internet misuse will be dealt with by the Head Teacher or a senior member of staff.* *Any complaint about staff misuse must be referred to the Head Teacher who should use the agreed SMBC procedures.* *Pupils and parents will be informed of the complaints procedure (see the school's Complaints Policy).* *Parents and pupils will need to work in partnership with staff to resolve issues.* *Sanctions for pupils within the school discipline policy include:* *> interview/counselling by head of year or senior leader;* *> informing parents or carers;* *> removal of Internet or computer access for a period.*