e-Safety Policy

Contents

Vision and Values

William Farr (C of E) Comprehensive School's vision is to provide all members of the school community with the opportunities to engage with 'life in all its fullness' (John 10:10) through the highest quality of education, encouragement and endeavour. We are committed to striving for excellence and ensuring that all students are known, valued and can achieve.

Our core values are:

Compassion; Friendship; Perseverance; Respect; Responsibility; Wisdom.

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents, etc.

SLT – Senior Leadership Team at William Farr Church of England Comprehensive School

WFS – William Farr Church of England Comprehensive School

AUP – The Acceptable Use Policy

Safeguarding is a serious matter; at WFS, we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such, this policy will be reviewed on a regular basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the WFS intranet; upon review all members of staff will sign as read and understood both the e-safety policy and Staff the Acceptable Use Policy. Upon return of the signed permission slip for students and the AUP for staff and acceptance of the terms and conditions, students and staff will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such, they will:

- Review this policy regularly and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- One governor will be delegated overall responsibility for Child Protection and e-safety is a crucial part of this role, the Governor will:
    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to two members of staff, the e-Safety Officers, as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officers have has had appropriate CPD in order to undertake the day-to-day duties.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Officers

The day-to-day duty of e-Safety Officer is devolved to Mrs Helen Bates who is the Designated Safeguarding Lead (DSL) and Mrs J Hazzledine (Associate Head Teacher).

The e-Safety Officers will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the SLT
- Advise the Headteacher, SLT, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical staff
- Make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher, SLT and responsible governor to decide on what reports may be appropriate for viewing.
- Where issues arise that are covered in the Safeguarding Policy they will be investigated appropriately using the Safeguarding Policy.

ICT Technical Staff

IT Technical Staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
    - Passwords are applied correctly to all users regardless of age. Passwords for staff will be standard high strength safe passwords i.e. a minimum of 8 characters, containing upper and lower case characters, numbers and special characters. Staff are asked to consider using a passphrase rather than a password. Staff passwords will be changed on a 6 monthly (180 day) basis.
    - The IT System Administrator password is to be changed on a three monthly (93-day maximum) basis.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher or a member of the SLT.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure, the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have access to the skills and knowledge they need to ensure the safety of children outside the school environment. WFS will keep parents up to date with new and emerging e-safety risks and online training or advice through the school website.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such, parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

WFS uses a range of devices including PC's and laptops. In order to safeguard the student and in order to prevent loss of personal data, we employ the following assistive technology:

Internet Filtering – we use WatchGuard® prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The IT Technical Staff and e-Safety Officers are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use WatchGuard®/ Microsoft filtering to prevent any infected email from being sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data. Spam email includes email where there is a phishing message.

Encryption – All school devices that hold personal data (as defined by the General Data Protection Act 2018) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher or SLT immediately. The schools GDPR Officer will liaise with the appropriate authorities to ascertain whether a report needs to be made to the Information Commissioner's Office.
(Note: Encryption does not mean password protected.)

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change if there has been a compromise. The IT Technical Staff will be responsible for ensuring that passwords are changed in these circumstances.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Technical Staff will be responsible for ensuring this task is carried out, and will report

to the Headteacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the Staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails. The use of personal email addresses for work purposes is not permitted.

Students are permitted to use the school email system, and as such will be given their own email address. The email address will involve their user name e.g 19jdoe@williamfarr.lincs.sch.uk

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic following of GDPR Policy guidelines, and is re-iterated here for clarity in the section titled 'The use of Images of Students in the school'.

All parents must sign a photo/video release slip; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; WFS is supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within WFS and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Headteacher and SLT for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Twitter – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such, no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- There is to be no identification of students using first name and surname; first name only is to be used.
- There is to be no student images used where the student can be identified without permission being sought from the parents or guardians, or the students themselves if they are over 14 years of age.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools' attention that there is a resource that has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day of the notification where possible. Where this is not possible, within a reasonable timeframe.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer(s), or in his/her absence the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, WFS will have an annual programme of training which is suitable to the audience.

E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will have impart positive messages about the safe use of technology and risks as part of the student's learning.

Safe Social Networking programme

As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area, this must be brought to the attention of the Headteacher for further CPD.

Acceptable Use Policy (AUP)

Guidelines for Staff

The school has provided computers for use by staff as an important tool for teaching, learning, and administration of the school. Use of school computers, by both members of staff and students, is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the Member of the Senior Team responsible for IT in the first instance.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the school's computer system may result in disciplinary action (including possible termination), and civil and/or criminal liability.

Please note that use of the school network is intended to be as permissive and flexible as possible under current UK legislation and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

Lastly, the school recognises that the distinction between computer use at work and at home is increasingly blurred, While the school neither wishes nor intends to dictate how you use your own computer, staff should consider that the spirit of this policy applies whenever you are undertaking an activity that stems from your employment with the school, however you are accessing it.

Computer Security and Data Protection

a) You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and it is for your use only. As such, you must not disclose your password to anyone.

b) It is assumed that ICT Techs know your password therefore you are not disclosing it

c) You must not allow a student to have individual use of a staff account.

d) When leaving a computer unattended, you must make every effort to either log off your account, or lock the computer to prevent anyone using your account in your absence (Press 'Windows Button' and L).

e) You must not store any sensitive or personal information about staff or students on any portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and approved for such use by the school.

f) You must not transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by the school.

g) When publishing or transmitting non-sensitive material outside of the school, you must take steps to protect the identity of any student whose parents have requested this.

h) If you use a personal computer, laptop or other device at home for work purposes, you must ensure that any school-related sensitive or personal information is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.

i) You must not make your own backup of data kept on any storage system other than the network storage drives or your Network Share N: drive. This includes USB memory sticks (even those owned or issued by the school) or a personal computer. You may back up documents etc; that do not include any school data.

j) You must ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored out of sight in a locked room or cupboard when left unattended. This includes at the end of the school day and overnight.

k) If taking school laptops etc; home, you should make every effort it is kept secure at home and during transport e.g. place it in the boot of a car, keep out of sight of onlookers etc;

l) Equipment taken offsite within the United Kingdom is routinely insured by the school. However you should make every reasonable effort to protect its security, and seek advice from the school prior to taking any device outside of the United Kingdom.

Personal Use

The school recognises that occasional personal use of the school's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use

a) must comply with all other conditions of this AUP as they apply to non-personal use, and all other school policies regarding staff conduct;

b) must not interfere in any way with your other duties or those of any other member of staff;

c) must not have any undue effect on the performance of the computer system; and

d) must not be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Use of your own Equipment

a) Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff or an external provider of such testing, and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.

b) You must not connect personal equipment to school network without prior approval from IT Network staff.

c) If you keep files on a personal storage device (such as a USB memory stick), you must ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation on harmful software onto the school computer system.

Conduct

a) You **must** at all times conduct your electronic device (including mobile phone) usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:

b) Use of mobile phones during meetings

c) Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;

d) Making ethnic, sexual-preference, or gender-related slurs or jokes.

e) You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.

f) You **must** not intentionally damage, disable, or otherwise harm the operation of computers.

g) You **must** make efforts not to intentionally waste resources. Examples of resource wastage include:

   i) Excessive downloading of material from the Internet;

   ii) Excessive storage of unnecessary files on the network storage areas;

h) You should avoid eating or drinking around computer equipment.

i) All use of the Internet is governed by a legal agreement with our Internet Service Provider (ISP) in addition to the guidelines here.

Use of Social Networking websites and online forums

Staff should not be using social media during the school day, even in free periods. Staff must take care when using social networking websites such as Facebook etc; even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any student to access personal information you post on a social networking site. In particular:

a) You **must not** add a current student to your 'friends list'.

b) Students who have left the school should not be contacted directly via a social network unless it is a site maintained by the school. Your union advises you not to contact students for up to 5 years.

c) You **must** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.

d) You should avoid contacting any student privately via a social networking website, even for school-related purposes.

e) You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff should also take care when posting to any public website (including online discussion forums, twitter or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

f) Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the school.

g) You should not post any material online that can be clearly linked to the school that may damage the school's reputation.

h) You **must not** post images or videos of current students on any social media (unless they are of your own child and no other students are visible in the post)

i) You should avoid posting any material clearly identifying yourself, another member of staff, or a student, that could potentially be used to embarrass, harass, or defame the subject.

Use of Email

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the school. This email address must not be used for anything other than school business. The following considerations must be made when communicating by email:

a) E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.

b) E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You **must not** purchase goods or services on behalf of the school via e-mail without proper authorisation.

c) All school e-mail you send should have a digital signature (this is a text signature) containing your name, job title and the name of the school.

d) E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the school.

e) Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users.

f) You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

g) Emailing students should only ever be from your school account and relate directly to school business.

h) Emailing any other person outside the school staff when in relation to school business should only be done via your school account; you should also take care not to forward emails to persons or companies outside the school to avoid exposing email addresses of other people, including other school staff without their permission.

Supervision of Student Use

a) Students in years 7 to 11 **must** be supervised at **all** times, (students in Resources are supervised by the librarian) when using school computer equipment. When arranging use of computer facilities for students, you must ensure supervision is available.

b) There is software available (AB Control) for all staff to allow them to view students computers to monitor their work and block website access etc;

c) Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for students is enforced.

d) Supervising staff **must** ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by students.

Privacy

a) Use of the school computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of computer use via our school network. In particular, the school does remotely monitor networked activities of both students and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.

b) You should avoid storing sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).

c) The school may also use measures to audit use of computer systems for performance and diagnostic purposes.

d) Use of the school computer system indicates your consent to the above described monitoring taking place

Confidentiality and Copyright

a) Respect the work and ownership rights of people outside the school, as well as other staff or students.

b) You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

c) You **must** consult a member of IT Technical staff before placing any order of computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's systems.

d) As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the business of the School or capable of being used or adapted for use within the School shall be immediately disclosed to the School and shall to the extent permitted by law belong to and be the absolute property of the School.

e) By storing or creating any documents or files on the school computer system, you grant the school a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit

Problems with the Computer System

a) It is the job of the IT Technical Team to ensure that the school computer system is working optimally at all times and that any faults arerectified as soon as possible. To this end:

b) You should report any problems that need attention to a member of IT Technical staff as soon as possible, including damage done to equipment. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone, the schools help desk; any other problem **must** be reported via the online help desk.

c) If you suspect your computer has been affected by a virus or other malware, you **must** report this to a member of IT Technical staff **immediately**.

d) If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable (mere minutes can count).

Reporting Breaches of this Policy

a) All members of staff have a duty to ensure this Acceptable Use Policy is followed. You **must** immediately inform a member of the IT Technical staff, or a member of the SLT, of abuse of any part of the computer system. In particular, you should report:

b) any websites accessible from within school that you feel are unsuitable for staff or student consumption;

c) any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;

d) any breaches, or attempted breaches, of computer security; or

e) any instance of bullying or harassment suffered by you, another member of staff, or a student via the school computer system.

f) Reports should be made either via email or the online Support Request system. All reports will be treated confidentially

Staff who are provided with Laptops

Where possible and appropriate, laptops or notebooks will be supplied to teachers and support staff for use both in and outside the school in order to enhance, enrich, and facilitate teaching and aid with administrative duties and school communications. The school's laptops and notebooks are to be used as a productivity tool for school-related business.

All laptops and related equipment and accessories remain the property of William Farr Church of England Comprehensive School at all times, and are provided to the staff members until such time as their employment with this school is terminated, when it must be returned. The school retains the right to remove such property from staff at any time should it be deemed necessary to do so by the SLT for reasons of security of school information and data and /or safety of students and staff. While the school's laptop computer is in their care, and as a condition of their use, staff members must comply with and agree to all of the following:

a) Prior to being issued one of the school's laptop computers, staff members will sign this Policy.

b) Insurance cover provides protection from the standard risks but excludes accidental damage and theft/loss that occurs off school premises. Staff members are expected to protect school laptops from damage and theft/loss and, as such, if the laptop sustains damage due to negligence on your part (on- or off-site), or is stolen, lost or damaged whilst off school premises, you will be responsible for its repair or replacement (at a cost to yourself).

c) Any damage that occurs to the laptop and/or any related equipment on- or off-site must be reported directly to a member of the Senior Leadership Team as soon as the damage occurs. If the laptop is deemed irreparable the school reserves the right to refuse a replacement machine.

d) Staff members should NOT attempt to install software or hardware or change the system configuration including network settings.

e) Staff members must provide access to any laptop computer, equipment, and/or accessories they have been assigned upon the school's request.

f) Only software licensed by the school, authorised by the IT Systems Manager and installed by the school's IT technical staff may be used.

g) Anti-Virus software (SOPHOS) is installed and is automatically be updated regularly.

h) Safeguarding monitoring software (SECURUS) will monitor activity on all machines linked to the schools network.

i) Should any faults occur the school's IT staff must be advised as soon as possible so that they may undertake any necessary repairs. Under no circumstances should staff attempt to fix suspected hardware or software faults, or make any configuration or system changes.

j) Any charges incurred by staff accessing the Internet from home are not chargeable to the school.

k) Local Authority and school policies regarding appropriate use, data protection, the freedom of information act computer misuse and health and safety must be adhered to by all users of the laptop.

l) Staff members are expected to exercise appropriate professional judgment and common sense when using the school's laptop computers on- and off-site.

m) The Laptop must be connected to the school network at least once every week during school term times, or more often if requested by the IT Technicians or SLT in order to back up work, receive any system updates and subject the laptop to virus checking.

n) Warrantee, licence or identifying stickers or labels must not be removed from the laptop.

Only the person to whom the lap top has been allocated should use the laptop the only exception is IT staff who will require access for maintenance issues.

Review and Evaluation

o) This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Notes

"Sensitive personal information" is defined as information about an individual that is protected by law under the General Data Protection Act 2018. Examples of such data include addresses and contact details of individuals, dates of birth, images and student SEN data. This list is not exhaustive. Further information can be found in the school's General Data Protection Policy.

Extract from the school website - Privacy Notice (How we use student information)

We collect and hold personal information relating to our students and may also receive information about them from their previous school. The school uses and processes student information within the remit of the Regulation (EU) 2016/679 (General Data Protection Regulation), referred to throughout this statement as the GDPR.

The categories of student information that we collect, hold and share include:

- Personal information (such as name, unique student number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as internal tests, students progress information and examination results)
- Medical information (such as allergies to food, medication a student may require and medical incidents that have occurred inside or outside of school that may affect learning)
- Special Educational Needs and Disabilities information (such as specific learning difficulties, specific medial needs and previous learning or medical needs)
- Behavioural information (such as rewards, achievements, incident slips and exclusions)
- Post 16 information (such as destinations data, UCAS applications and grants)

We also process special categories of personal data that may include:

- physical or mental health needs
- racial or ethnic origin
- criminal convictions data
- civil and criminal proceedings, outcomes and sentences
- religious or other beliefs of a similar nature

Why we collect and use this information

We use the student data:

- to support student learning
- to monitor and report on student progress
- to provide appropriate care and guidance
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use student information under Article 6 and Article 9 of the GDPR, this enables the school to process information such as assessments, special educational needs requests, Departmental Censuses under the Education Act 1996 and the Education Act 2005, examination results and other such data processes that relate educational data to the individual within the requirements for the school to provide education for the individual.

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

How do we collect your personal data?

Information may be collected in many different ways but predominantly as set out below:

Face to Face

If you attend our school or we visit you we may collect your personal data.

Telephone calls

Recordings may be used as evidence of the call and for our staff training, monitoring for abusive and quality purposes.

Emails

If you email us we may keep a record of your email address and the email as evidence of the contact. We are unable to guarantee the security of any email initiated by you and we recommend that you keep the amount of confidential information you send to us via email to a minimum.

CCTV

We have installed CCTV systems on our premises , for the purposes of public, student and staff safety and crime prevention and detection. Signs are displayed notifying you that CCTV is in operation and providing details of who to contact for further information.
We will only disclose CCTV images to others who intend to use the images for the purposes stated above. CCTV images will not be released to the media for entertainment purposes or placed on the internet. Images captured by CCTV will not be kept for longer than necessary.

Storing student data

We hold student data in line with our Data Retention Guidelines, which are available upon request.

Who we share student information with

We routinely share student information with:

- schools and other educational environments that the students attend after leaving us
- our local authority
- the Department for Education (DfE)
- the Police and Law Enforcement
- the School Nursing Team
- the National Health Service
- our Careers Advisory Service
- our Educational Welfare Officer
- The specialist Schools and Academy Trust
- The Princes' Teaching Institute
- Examination Boards

Why we share student information

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our students with the (DfE) under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

Students aged 13+

Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / student once he/she reaches the age 16.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Students) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided student information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the schools GDPR Manager

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

The use of Images of Students in the school

Photographs, Video and the use of Media relating Students

To celebrate the achievements of our students and students we obviously wish to display photographs and information about the wide range of activities with which they are involved. This is will recognise their personal success, but will also generate enthusiasm and motivate others. These displays may be internal on notice boards, as part of an article in Farrago, the school newsletter, the school brochure, or externally in the local and national media and on our website either by our own submission of information or more often by the way of photographs and interviews.

Parents may be reassured that whenever we are requested by the press and other media for information about our students activities, including photographs and interviews any decision to go ahead made by a senior member of staff and if agreed, are always carried out with a member of staff present. Great care is always taken to ensure that individual's name and details are only displayed where appropriate.

Unless parents inform us otherwise, given the above safeguards, we believe that is reasonable for us to assume that they will have no objection to this limited use of images and information.

The training of staff and the monitoring and evaluation of staff teaching and student learning has always been of importance in the drive to develop expertise and improve the overall quality of the education we provide. Technological advances have now provided greater opportunities by the way of the observation of lessons in a non-intrusive way through the use of video camera/recording/playback facilities and with the necessary

agreements and protocols in place, we wish to take advantage of this new equipment and the opportunities it provides. Previous pilot projects show us that students are very willing to be involved.

Parents must give consent before images can be taken or used in any manner. Students over the age of 14 years may give permission for their own image to be taken or used. An absence of consent must be taken as an objection to images being taken or used. Staff must check whether students have this consent in place before any activity where images may be recorded occurs, and take steps to prevent this happening during the event if consent is not in place or has been refused.

Parents give permission on the Emergency Contact Form, which is submitted as students join the school. (See Appendix 2 for an extract of this form illustrating this). This information may be viewed by staff on our Management Information System (Progresso). Students over the age of 14 can give their permission using the student consent form (See Appendix 2).

Appendix 1 – Network Code of Conduct (Student version):

WILLIAM FARR

C of E Comprehensive School

Agreed Information Technology Code of Conduct for using the Network, Internet and e-mail at school.

Please read the following points carefully and make sure that you understand everything before signing the consent form. Students granted access to the school network, including e-mail, will abide by the IT Code of Conduct.
All users of the Network and Internet are expected to abide by these rules of computer and network use.

- Be polite when using e-mail. Do not use e-mail to bully or insult others.
- Do not use inappropriate or unacceptable language.
- Never reveal your personal address or telephone number or those of fellow students to people unknown to you.
- e-mail is monitored by the school security system. Never say anything or engage in anything that you would not be happy to write on a postcard that could be read by everyone.
- Inform a member of staff IMMEDIATELY you discover an obscene or offensive web page so that its access can be blocked.

Students agree that they will **NOT PERFORM** the following unacceptable actions:

- Try to bypass the internet security.
- Complete questionnaires or subscription forms without checking with a member of staff.
- Damage, degrade or disrupt the performance of equipment or systems.
- Attempt to retrieve information about 'hacking' or attempt to 'hack' our system.
- Download programmes.
- Play computer games unless they have permission from their teacher to play subject based games / learning activities as part of the curriculum.
- Send or display offending messages, pictures, videos or sound.
- Use the internet to buy or sell anything.
- Use the internet to access obscene or offensive web pages/material.
- Use the network for any illegal activity, including the violation of copyright or other laws.
- Use someone else's account, either with or without permission.
- Waste printer paper.
- Tell another student your password.

The school will electronically audit your Internet and e-mail usage at all times and a record of this is kept.

Student and parent/guardian consent:
No student will be granted access to the Internet without both student and parent/guardian signing the Code of Conduct consent form.

The consent form allows parents/guardians to confirm that their child may or may not have access to the Internet.

The consent form confirms that the student has read and agrees to abide by the Code of Conduct.

Agreed Information Technology Code of Conduct for using the Network, Internet and e-mail at school

Student Name: _____

Form _____

Username if known: _____

Student Consent Form

I have read and agree to abide by the IT Code of Conduct in both letter and ethos. I understand that breaching the Code will result in the sanctions by the school.

Student signature: _____

Parent/Guardian Consent Form

I understand that my child now has the opportunity to have access to the Internet and an e-mail address. I have read the school's IT Code of Conduct and *grant/do not grant my permission for my child to have access to the Internet and e-mail.

Signed: _____

Date: _____

Print Name: _____

*Delete as appropriate

Appendix 2 – Parental and Student Consent for use of images:

Parental consent – extract from the Emergency Contact Form:

MODE OF TRAVEL	☐ CAR/VAN ☐ TAXI	☐ DEDICATED SCHOOL BUS ☐ PUBLIC SERVICE BUS	☐ WALK ☐ CYCLE	☐ OTHER
RELIGION		ETHNICITY		
LANGUAGE SPOKEN AT HOME (IF NOT ENGLISH)		NATIONALITY		
ARMED SERVICES CHILD (PARENTS WITHIN THE LAST SIX YEARS) PLEASE SUPPLY EVIDENCE				YES / NO
I GRANT PERMISSION FOR THE SCHOOL TO ACQUIRE AND PROVIDE CAREERS ADVICE DURING THE TIME IN SCHOOL				☐ YES ☐ NO
I GRANT PERMISSION FOR THE SCHOOL TO USE PHOTOGRAPHIC IMAGES IN LINE WITH THE SCHOOL'S POLICY				☐ YES ☐ NO

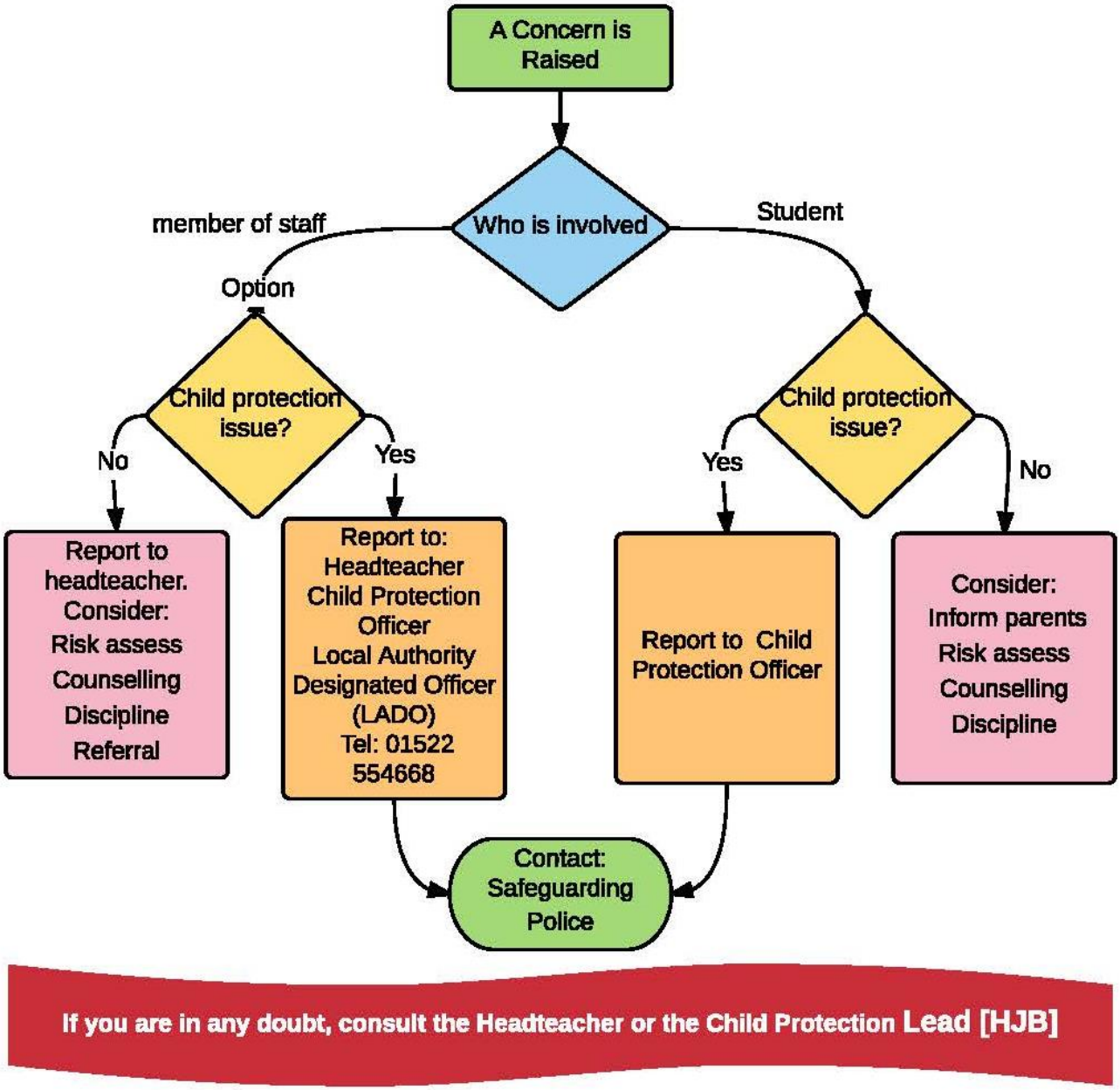
Student Consent Form – For use with students over 14 Years of age:

William Farr School Student Consent Form – Images
As part of your experience in our school there will be many events and activities that we would like to celebrate with others. When these happen, we will often take pictures and videos to celebrate what you have done as an individual or in a group, and also to encourage others to join in. We may use these images on displays in school e.g. on screens, or on notice boards, as part of an article in the school newsletters, the school brochure, or in the local and national media and on our website. (When we are asked by the press or other media for information about student activities, including photographs and interviews, any decision to go ahead made is by a senior member of staff and if agreed, they are always carried out with a member of staff present. We will make sure that student names and details are only displayed where it is needed.) **Please write your name and sign below if you agree for this to happen.**
Student name (please write clearly)
Signed:
Date:

Appendix 3 – E-Safety incident log to record incidents:

Number:	**Reported By:** (name of staff member)	**Reported To:** (e.g. Head, e-Safety Officer)	
	When:	When:	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		Date:	
Signature (Governor)		Date:	

Appendix 4 Inappropriate Activity Flowchart:



Appendix 5 - Illegal Activity Flowchart (actions for Safeguarding Lead):