E-SAFETY POLICY

Introduction and Overview

At The Laurels School, we are committed to safeguarding and promoting the welfare of all pupils in our care. Our e-safety strategy enables us to create a safe e-learning environment that:

- Promotes the teaching of IT within the curriculum
- Protects children from harm
- Safeguards staff in their contact with pupils and their own use of the internet
- Ensures the school fulfils its duty of care to pupils
- Provides clear expectations for all on acceptable use of the internet

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at The Laurels School with respect to the use of online-based technologies.
- Safeguard and protect the children and staff of The Laurels School.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact

Being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct

Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying

Commerce

Risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Policy Scope

This policy applies to all members of The Laurels School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of The Laurels School.

The Education and Inspections Act 2006 empowers the Headmistress to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

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

Roles and Responsibilities for online safety

Teaching e-safety

One of the key features of our e-safety strategy is teaching pupils to protect themselves and behave responsibly while online. The Computer Science teacher has overall responsibility for the coordination of e-safety education, but all teaching staff play a role in delivering e-safety messages. Staff are aware that it is important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching can be built into existing lessons across the curriculum, covered within specific online safety lessons and/or school wide approaches. Teaching must always be age and developmentally appropriate. Pupils are taught how to evaluate what they see, how to recognise techniques used for persuasion, online behaviour, how to identify online risks and how and when to seek support:

- The benefits and risks of using the internet
- How their behaviour can put themselves and others at risk
- What strategies they can use to keep themselves safe
- How to build resilience to protect themselves and their peers
- What to do if concerned about something they have seen on the internet
- Who to contact with concerns
- That the school has a 'no blame' policy so pupils are encouraged to report any e-safety incidents
- The school has a 'no tolerance' policy regarding cyber bullying
- That behaviour that breaches acceptable use will be subject to sanctions and disciplinary action. In the event that a pupil accidentally accessed inappropriate materials they must report this to an adult immediately and take appropriate action to hide the screen or close the window so that an adult can take the appropriate action. Where a pupil feels unable to disclose abuse, sexual requests or other misuses against them to an adult they can use the Report Abuse button (https://www.thinkuknow.co.uk/ or ceop.police.uk) to make a report or seek further advice.

Delivering e-safety messages to the school community

- Y7 and all new pupils are given an IT Induction which includes elements of E-Safety, internet use and how to keep safe online.
- Staff complete Educare E-Safety and Cybersecurity courses.
- Pupils receive ongoing E-Safety education as part of Character Education and in Assemblies e.g. for Safer Internet Day
- The Computer Science teacher is responsible for delivering on-going e-safety education in the classroom through taught computer science lessons (see Appendix 1 for KS3 National Curriculum) and ensures that they are up-to-date with current practice.
- Reminders are given periodically regarding the expectations on internet use and how to keep safe
- Firewalls are in place to ensure that pupils are accessing suitable age appropriate sites
- Monitoring of internet usage by pupils and staff is ongoing.

Evaluating and using internet content

Teachers encourage and teach good internet research skills. This includes critically evaluating retrieved information by:

- Questioning the validity of the source of information
- Comparing alternative sources of information
- Understanding the implications of copyright, correctly quoting sources and that plagiarism is unacceptable.

Pupils with special needs

Pupils with learning difficulties and/or any disabilities may be more vulnerable to risk from use of the internet and require additional guidance on e-safety practice as well as closer supervision. The SENCO should ensure that the school's e-safety policy is adapted to suit the needs of pupils with special needs. They need to liaise with parents and other relevant agencies in developing e-safety practices for pupils with special needs and to keep up to date with any developments regarding emerging technologies and e-safety and how these impact on pupils with special needs.

The Laurels School pupil e-mail accounts

Pupils are taught about their e-mail account usage as part of the IT induction and IT use across the curriculum. The following areas are covered:

- Pupils are taught not to disclose personal contact details via e-mail correspondence
- All e-mail communications should be polite and if a pupil receives an offensive e-mail, they should not reply but tell a teacher immediately
- Pupils should be aware that bullying via e-mail will not be tolerated and will be dealt with in accordance with the Anti-bullying policy
- Pupils are made aware that the use of their school e-mail is for educational purposes only
- Pupils should not open attachments if they are unsure of the content or have no knowledge of the sender

Mobile / SMART Technology

Children now have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G), which some them may abuse to sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. Awareness of the dangers are detailed in TLS Procedures in Appendix 3.

Social Networking

The widespread availability and use of social networking bring opportunities to understand, engage and communicate with the outside world in new ways. It is important that pupils are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that our legal responsibilities and our reputation are upheld to the highest standards. For example, use of social networking applications has implications for the duty to safeguard pupils.
Some examples of social networking applications are:
Snapchat, Blogs, Online discussion forums, Collaborative spaces, Media sharing services e.g. Youtube, 'Micro logging' applications e.g. Twitter, Virtual worlds – MMORPG (Massive Multiplayer Online Role Playing Games – e.g. World of Warcraft, Runescape)

All incidents of complaints relating to e-safety and unacceptable internet use must be reported to the Head and the Designated Safeguarding Lead (DSL) immediately. Where relevant this will be recorded.

In the unlikely event a pupil unintentionally opens a website with distressing or inappropriate content, teachers should immediately close the screen, reassure the pupil that they have done nothing wrong and report the details of the website to the IT Services Manager who will then ensure that the site is blocked.

Again, although unlikely (due to internet filters on our server), if a pupil *intentionally* accesses an inappropriate website they will be subject to the sanctions set out in the Behaviour Policy.

Cyber Bullying

Cyber bullying is defined as the use of technology to deliberately hurt or upset someone. The internet allows bullying to continue past school hours and invades the victim's home life and personal space and allows for hurtful comments and material to be available to a wider audience.

Bullying may take the form of:

- Rude, abusive or threatening messages via e-mail, text or social networking sites (as listed above)
- Posting insulting, derogatory or defamatory statements on blogs or social networking sites
- Setting up websites that specifically target a victim
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or email
- Cyber bullying can affect both pupils and staff and it could be deemed a criminal offence
- Incidents of cyber bullying are reported to the Head or DSL and if extreme may in turn be reported to the police

All website providers and mobile phone companies are aware of the issue of cyber bullying and have their own systems in place to deal with problems, such as tracing and blocking communications and will give advice to parents and teachers. Parents should be notified of any such incidents so they can block any

offensive messages on home computers.

Working with Parents

This policy is published on the school website and parents are asked to sign the 'Acceptable Use Policy' together with their daughter as part of the admissions process. Pupils review this agreement and sign again at the completion of their IT Induction, a copy of which is sent to their school pupil email account. Information about e-safety is shared with parents via our Digital Safety page under the Parents tab on our school website. This page is maintained by the IT Services Manager and emails are sent to parents with relevant articles or guidance when appropriate or in response to topical events in the media.

Role of staff

All staff are responsible for ensuring they do not personally access inappropriate content on the internet whilst at school. They are also responsible for managing personal data in line with statutory requirements. Refer to our Staff Code of Conduct for further information under our Policies tab on our school website.

The Head has ultimate responsibility for e-safety issues within the school including:

- Implementation of the school's e-safety policy (this policy)
- Ensuring that e-safety issues are given high profile
- Linking with governors, parents and staff to promote e-safety
- Ensuring e-safety is embedded in the curriculum
- Deciding on sanctions against staff and pupils in breach of policies

Role of Designated Safeguarding Leads (DSLs)

Any e-safety issues which may have serious implications for a child's safety should without delay be referred to the DSL and the IT Services Manager. Advice will be sought from the Croydon Safeguarding Children Partnership if escalation is required.

Role of Governing Body

As governing bodies have a statutory responsibility for pupil safety, it is vital that governors are aware of e-safety issues and support the Head in the development of the e-safety strategy and promoting e-safety to parents. Maria Kemp, as the school's Safeguarding governor, has responsibility for this area.

Education and Curriculum

This school has a clear, progressive e-safety education programme as part of the IT curriculum and the Character Education Programme. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK

- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- To know how to narrow down or refine a search;
- To understand how search engines work and to understand that this affects the results they see at the top of the listings;
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- To understand why they must not post pictures or videos of others without their permission;
- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- To understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. from a parent or carer, teacher or trusted staff member, or an organisation such as thinkuknow.co.uk

The curriculum strategy ensures:

- Careful planning of internet use ensuring that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Staff model safe and responsible behaviour in their own use of technology during lessons.
- That when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- That staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection ensuring GDPR compliance;
- Makes training available where required to staff on e-safety issues and the school's e-safety education programme.
- Provides, as part of the induction process, all new staff with information and guidance on the e-safety policy and the school's Acceptable Use Policies.

Parent awareness and training

This school provides advice and guidance for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safety behaviour are made clear
- Digital Safety page on the school web site
- Demonstrations, practical sessions held at school
- Suggestions for safe Internet use at home;
- Provision of information about national support sites for parents.

Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school systems in accordance with the Acceptable Use Policy which they will be expected to digitally sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices (see guidance from Parent/Staff Handbook in Appendix 3). They should also know and understand school policies on the taking / use of images and on cyber bullying

Staff

- Are responsible for reading the school's e-safety policy and using the school IT systems accordingly, including the use of mobile phones, and handheld devices.

Pupils

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Sign a 'responsible ICT use' agreement at the beginning of their time in school

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions – where an incident occurs, the guidelines of our behaviour policy are followed.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (eg. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- Monitoring and reporting of e safety incidents takes place and contributes to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

School website and Social Media

The Head takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

- Uploading of information is restricted to our website administrators;
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.
- Our Facebook and school Twitter accounts are managed by our Admissions Officer. The same principles as for the website are applied.

Filtering and monitoring

Network access for all connected devices is logged and filters are in place to limit or block traffic where appropriate; this includes blocking illegal, potentially harmful sites, and decryption of secure websites (for the purposes of filtering and security). It should be borne in mind that this is not always technically possible, and methods of sidestepping school protections (VPNs etc) are a constant possibility, despite being contrary to AUPs.

The school implements keyword and artificial intelligence filtering across a broad spectrum of categories including cyber-bullying, self-harm and grief. Automatic block lists are updated daily by the system provider of the web filter, which ensures where possible that lists of illegal or potentially harmful websites are kept up to date, as well as manually blocking specific websites or applications that are considered harmful or inappropriate by the school.

The following categories are blocked by our broadband provider (LGFL) across all year groups outside age-appropriate restrictions:

- **Discrimination**. Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.
- **Drugs / Substance abuse.** Displays or promotes the illegal use of drugs or substances
- **Extremism**. Promotes terrorism and terrorist ideologies, violence or intolerance

- **Malware / Hacking.** Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- **Pornography**. Displays sexual acts or explicit images
- **Piracy and copyright theft.** Includes illegal provision of copyrighted material
- **Self Harm.** Promotes or displays deliberate self harm (including suicide and eating disorders)
- **Violence.** Displays or promotes the use of physical force intended to hurt or kill

It is recognised that there may be occasions when, for good educational reasons, students and staff may need to access content that is normally blocked. When this happens, a request may be submitted to the IT Helpdesk for consideration.

In consultation, the IT Manager, IT Services Coordinator and the DSL review the internet filtering rules termly. A copy of the filtering checklist can be found at the end of this policy - Appendix 4. Also, the school internet filtering and monitoring systems provide information and alerts on students' network activity and behaviour that might constitute a safeguarding concern. The DSL reviews this information termly, however any potential concerns that have been highlighted by the IT Manager or the IT Services Coordinator are investigated fully in partnership with the DSL and appropriate action is taken.

When children use the school's network to access the internet, they are protected from inappropriate content by our filtering and monitoring systems which are regularly reviewed for their effectiveness. However, many pupils are able to access the internet using their own data plan. Online safety training is integrated, aligned, and considered part of the whole school safeguarding approach and wider staff training and curriculum planning. It is also a component of new staff induction. All pupils are taught about safeguarding, including online safety. Our approach to online safety is broad, relevant, and tailored to the concerns and risks of particular age groups. It is delivered through a combination of the school curriculum, the Character Education Programme, assemblies, and outside speakers, which, together with the Acceptable Use Policy, aims to develop safe and responsible behaviour both within and outside school.

Appendix 1 - PUPIL Guidelines for remote learning

Virtual Classroom Framework

In the event that the school is advised to close, remote learning will provisioned mainly by utilisation of our existing online learning platform – Google Education Suite. Our school google domain @thelaurelsschool.org enable each pupil to have a Laurels School google account. They can then access their online lessons through the following means:

- Google Classroom - where pupils can access each of their subjects via a virtual classroom.
- Google Drive – where pupils can store their documents.
- Google Email – where pupils can communicate with teachers and vice versa

Other VLE's (Virtual Learning Environments) include:

- Sciences – Kerboodle
- Maths – MathsBuster & MathsWatch
- MFL (Modern Foreign Learning) – Dynamic Learning (KS5) and ActiveLearn (KS3 & KS4)
- YouTube - either generated by the subject teacher or selected from the wider community to support a topic/lesson.

Video conferencing (to enable you to join a classroom and see the teacher) will be delivered via Zoom and/or Google Meet. Further guidance will be given if and when Remote Learning is required.

FAQ's for remote learning pupils

Q: Should I expect my teachers to communicate to me via my google classroom and/or email?

A: Each teacher will let you know how they will be setting their work. We expect pupils in all year groups to read and follow the instructions which will be placed in the appropriate google classroom stream NOT your email.

Q: Do I need to be working during the normal school day?

A: Yes, you are expected to follow your timetable. For lessons where you may not have been set work on google classroom e.g. PE, this is an ideal opportunity for 1-2-1 support via conferencing with subject teachers or revising for your end of year exams.

Q: Do I need to submit/turn-in work?

A: Yes, you are expected to complete and submit/turn-in work set on google classroom as per teacher instructions and the specified deadline. Please expect consequences if you do not manage to do this (without a very good reason).

Q: If I feel there is too little/much work being set or feedback given – what should I do? A: Please contact your tutor by email in the first instance and explain the situation.

Q: Should I expect to be set work in all subjects?

A: Yes, you should expect to receive work in almost all subjects. You will know this via the google classroom stream.

Q: How will I know when the school re-opens?

A: This will be communicated to you and your parents via email.

IT Support

Q: I don't have a computer/laptop at home, what should I do?

A: Whilst we cannot provide a laptop to every teacher in the school, we can try to accommodate those in

most need. Please contact Mrs McManamon, IT Services Manager lara.mcmanamon@thelaurelsschool.org

Q: I have forgotten my school google password or any other VLE account, what should I do? A: Please contact Mrs McManamon, IT Services Manager lara.mcmanamon@thelaurelsschool.org

Q: I don't see my google classroom?

A: Email the subject teacher in the first instance for the classroom code.

Q: I have received a link but it does not work?

A: First check you do not have a block on pop-ups in your internet settings. If that does not resolve the issue, then contact Mrs McManamon, IT Services Manager, lara.mcmanamon@thelaurelsschool.org and copy in the teacher who sent the link so they are aware.

Q: I cannot get my computer/laptop to work. Error messages are displayed, or it says a link broken.

Please complete the following "housekeeping" tasks on your device and if you are still experiencing problems, contact Mrs McManamon, IT Services Manager, lara.mcmanamon@thelaurelsschool.org

1) Make sure your laptop/PC is up to date with latest updates and update if not, set to auto update for the future.

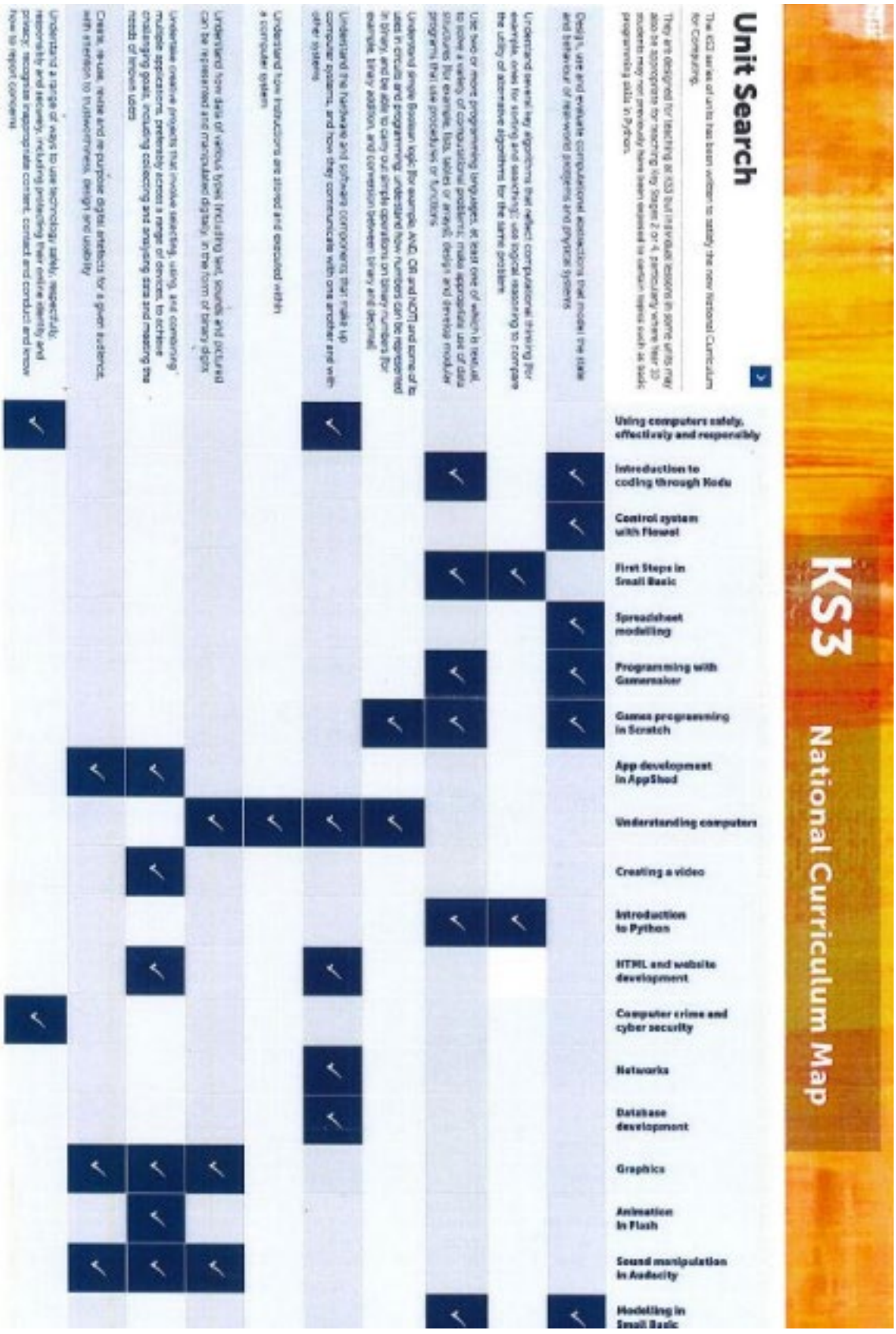
2) In your google chrome, clear your cache/history (holding down Ctrl + H whilst in Chrome is the shortcut). IMPORTANT! Please remember to untick the Password box otherwise you will lose all your saved passwords.

3) Shut down your laptop/computer EVERY night.

4) Make sure you have anti-virus software on your device such as Macafee.

5) You should where possible use a PC/laptop to run Zoom as it runs slightly differently to a phone. The teacher usually expects the camera and audio enabled at least when giving out instructions, beginning and end of lessons.

Appendix 2 – KS3 National Curriculum



Appendix 3

Guidance on Electronic Devices from Staff and Parent Handbooks

iPods, MP3 players, cameras and similar items may not be brought into school unless requested by a teacher for use in lessons. They will be confiscated if seen elsewhere in school (whether in use or not). Unauthorised

photography by pupils (with mobile phones or other devices) is prohibited. Laptops signed off by the IT Services Manager for use in school are the exception. Pupils are not allowed to carry mobile phones during the school day. Mobile phones will need to be stored in lockers from 8.30am until 3.45pm, (unless pupils are attending a co-curricular activity, in which case the mobile phone will need to be stored away until 5.15pm). They must be turned off and must not be used during break, lunchtime or at the beginning or end of the school day whilst the pupils are on the school site. In order to ensure that the rules on mobile phones are successfully implemented, we will instigate the following consequences if rules are infringed: the mobile phone will be confiscated and looked after safely in school. The phones will be returned after five school days. Pupils are not allowed to remove the SIM card or battery prior to confiscation. Parents are therefore asked not to contact their children in school on their mobile phones. In an emergency, the appropriate procedure for parents to relay urgent messages to pupils is through the School Office/Reception. A message will then be delivered to the pupils to come to Reception. If pupils do bring such items into school, they do so at their own risk. The school will not be responsible for any losses.

Appendix 4

Filtering and Monitoring

Whilst considering our responsibility to safeguard and promote the welfare of our pupils, we are doing all that we reasonably can to limit children's exposure to the above risks from the School's IT system. As part of this process, the School ensures we have appropriate filtering and monitoring systems in place and regularly review their effectiveness. We ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The school:

- Has identified and assigned roles and responsibilities to manage filtering and monitoring systems.
- Reviews filtering and monitoring provision at least annually.
- Blocks harmful and inappropriate content without unreasonably impacting teaching and learning.
- Has effective monitoring strategies in place that meet our safeguarding needs.

Document Title	E-Safety Policy
Version	V 2.0
Date	Summer Term 2023
Author	Lara McManamon and Vicky Sumner

Approved by Head Teacher	Yes
Approved by SMT	Yes
Approved by Safeguarding Governor	Yes
Next Review	Summer Term 2024