Gossops Green Primary School

The Collegiate Trust
Exceptional Education for All

Online Safety Policy

Approved by: LGB
Last Reviewed on: December 2022
Next review due by: December 2023
Staff Member Responsible: Designated Safeguarding Leader
Link Governor: Mr Toby Bartholomew

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including pupil personal electronic mobile devices
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk:

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils'

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

3.1 The Local Governing Body (LGB)

The Local Governing Body has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Local Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Governor who oversees online safety is: **Mr Toby Bartholomew**

All Governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all'

approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) [and deputies] are set out in our Safeguarding Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, *The Collegiate Trust* Director of IT, Computing Subject Leaders and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school Safeguarding policy
- Ensuring that any online safety incidents are logged (on CPOMS with the correct tag) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or Local Governing Body

This list is not intended to be exhaustive.

3.4 The Collegiate Trust (TCT) Director of IT

The Director of IT is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's computing systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety incidents are logged (on CPOMS with the correct tag) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's computing systems and the internet (appendix 2), as well as the Staff Code of Conduct and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (on CPOMS with the correct tag) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's Computing systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and Members of the Community

Visitors and members of the community who use the school's computing systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2) – depending on their level of access.

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum including in PSHE:

National Curriculum computing programmes of study.

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The use of *Safe* search engines such as Swiggle are encouraged (and promoted in the pupil Computing Charter) to reduce the risk of exposure to inappropriate sites and images.

The safe use of social media and the internet will also be covered in other subjects such as PSHE where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating Parents/Carers about Online Safety

The school will raise parents' awareness of internet safety in Newsletters or other communications home, and in information via our website.

This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

Parents will be informed of:

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with the Principal, DSL or Computing Leaders.

6. Cyber-Bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Behaviour policy.)

6.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will record the incident and if appropriate, report the incident to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining Pupil's Mobile Electronic Devices

The Principal, and any member of the Senior Leadership Team, authorised to do so by the Principal (as set out in our Behaviour Policy) can carry out a search and confiscate (as set out in our Pupil Personal Electronic Devices Policy) any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified as a breach in the Pupil Personal Electronic Devices Policy for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before searching a device, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Contact the parents/carers
- Make an assessment of how urgent the search of the device is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from [the Principal or DSL]
- Explain to the pupil why their device is being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to Principal or DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

All confiscations of devices will be recorded on CPOMS that day.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Behaviour Policy and Pupil Personal Electronic Devices Policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and Governors are expected to sign an *Acceptable Use Agreement* regarding the use of the school's computer systems, software and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Staff only have access to the school Wifi via a school device (signed in with their school user login) or via their own device on the *Bring Your Own Device* (BYOD) network, also only accessible with their school user login)

The Collegiate Trust IT Department will monitor the websites visited by pupils, staff, volunteers, Governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils Using Mobile Devices in School

Pupils in Yr5 and Yr6 only may bring mobile devices into school – once they have returned a completed *appendix A – Mobile Phone Acceptable Use Agreement* (from the Pupil Personal Electronic Devices Policy) to their class teacher. However, all mobile devices must be turned off (not simply silenced) upon entering the school grounds and pupils cannot use them on site, see school Pupil Personal Electronic Devices Policy.

Pupils do not have access to the school Wifi.

Any breach of the Mobile Devices Policy by a pupil may trigger disciplinary action in line with the school Behaviour policy and Mobile Devices Policy, which may result in the confiscation of their device.

9. Staff Using Work Devices and Accounts Outside School

All staff members will take appropriate steps to ensure their school devices and accounts remain secure, following the TCT ICT Policy. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g., asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not saving school data to their own device
- Sharing a device among family or friends that has school data or access to school accounts

Staff members must not use the device in any way which would violate the school's Acceptable Use Agreement, as set out in appendix 2.

If staff have any concerns over the security of their device, they must seek advice from the Director of IT or the IT Support Team.

10. How the School will Respond to Issues of Misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies;

- Behaviour Policy
- Pupil Personal Electronic Devices Policy
- Computing Charter

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the TCT Staff Policy and the Staff Code of Conduct and/or the Teacher Standards. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, weekly bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL [and deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding Policy.

12. Monitoring Arrangements

The DSL (and all staff) log behaviour and safeguarding issues related to online safety on CPOMS with the correct tag.

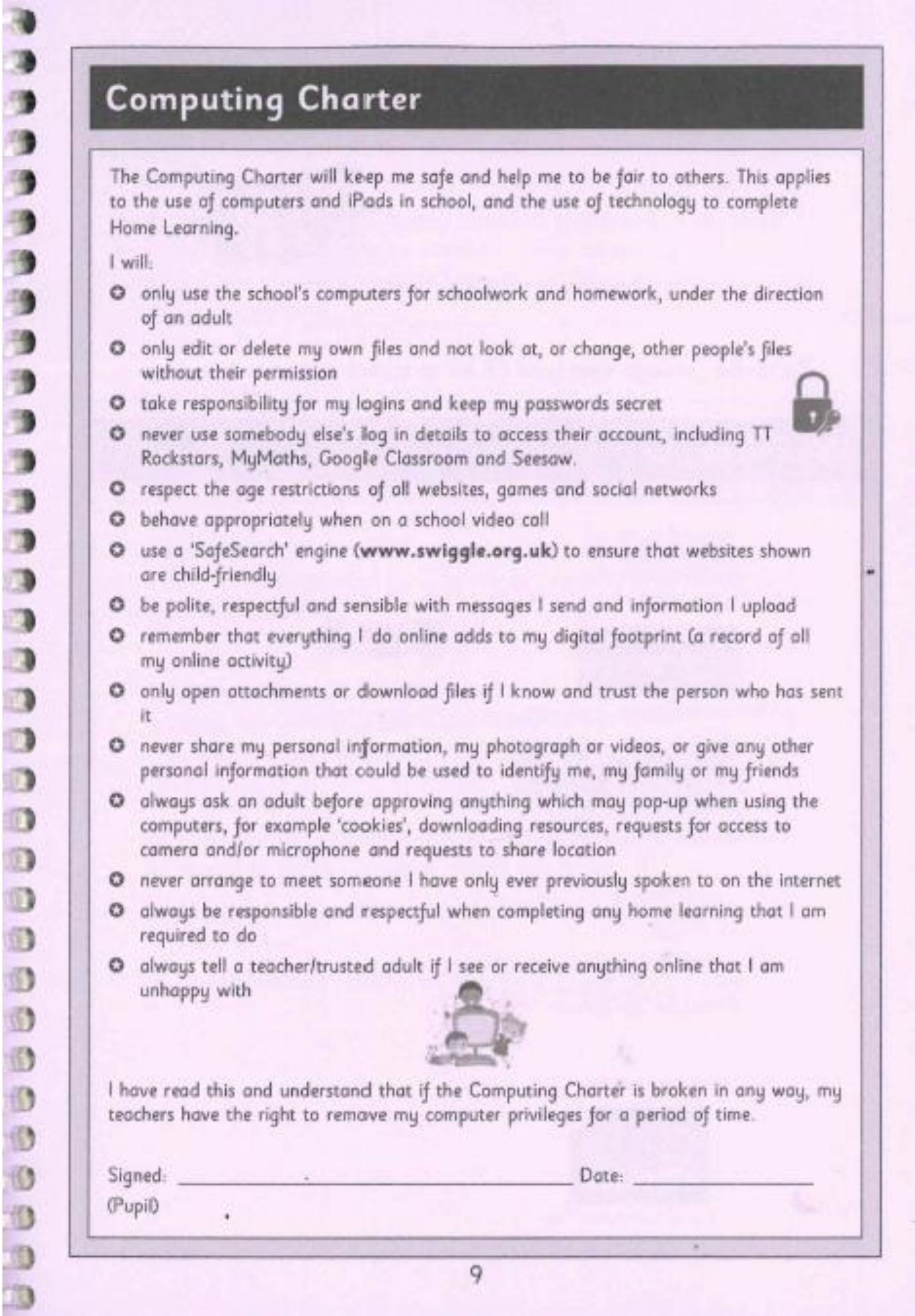
This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Governing Board. The review (such as the one available here) will consider and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This Online Safety Policy is linked to our:

- Pupil Computing Charter (in Home-School Diaries)
- Pupil Personal Electronic Devices Policy
- Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- TCT Staff Disciplinary Policy
- TCT Data protection policy and privacy notices
- TCT Complaints procedure
- TCT ICT Policy

Appendix 1: Pupil Computing Charter (Acceptable use Agreement)



Computing Charter

The Computing Charter will keep me safe and help me to be fair to others. This applies to the use of computers and iPads in school, and the use of technology to complete Home Learning.

I will:

- only use the school's computers for schoolwork and homework, under the direction of an adult
- only edit or delete my own files and not look at, or change, other people's files without their permission
- take responsibility for my logins and keep my passwords secret
- never use somebody else's log in details to access their account, including TT Rockstars, MyMaths, Google Classroom and Seesaw.
- respect the age restrictions of all websites, games and social networks
- behave appropriately when on a school video call
- use a 'SafeSearch' engine (**www.swiggle.org.uk**) to ensure that websites shown are child-friendly
- be polite, respectful and sensible with messages I send and information I upload
- remember that everything I do online adds to my digital footprint (a record of all my online activity)
- only open attachments or download files if I know and trust the person who has sent it
- never share my personal information, my photograph or videos, or give any other personal information that could be used to identify me, my family or my friends
- always ask an adult before approving anything which may pop-up when using the computers, for example 'cookies', downloading resources, requests for access to camera and/or microphone and requests to share location
- never arrange to meet someone I have only ever previously spoken to on the internet
- always be responsible and respectful when completing any home learning that I am required to do
- always tell a teacher/trusted adult if I see or receive anything online that I am unhappy with

I have read this and understand that if the Computing Charter is broken in any way, my teachers have the right to remove my computer privileges for a period of time.

Signed: ______________________________ Date: ______________
(Pupil)

9

Appendix 2: Staff Acceptable Use Agreement

From Staff Code of Conduct:

Appendix B – Acceptable Use Agreement – September 2022

- As a school user of the network resources, I agree to follow the school and The Collegiate Trust rules (set out in the *School Code of Conduct*, *Staff Handbook* and *Online Safety Policy* and in the associated Trust and school policies) on their use. I will use the network, hardware and Wi-Fi connections in a responsible way and observe all the restrictions explained in the associated school policies. If I am in any doubt, I will consult the IT Support Team
- I agree to report any misuse of the network to the IT Support Team and the Principal/Deputy Principal
- I agree to report any websites that are available on the school Internet that contain inappropriate material to the IT Support Team and the Principal/Deputy Principal
- I agree to use Social Networking in line with the guidance set out in the *Staff Code of Conduct Policy*.
- I agree to ensure that portable equipment such as laptops, iPads or cameras (and any other school equipment) will be kept secured when not in use and to report any misplacement or loss to the Principal/Deputy Principal (who will report it to the TCT IT Support Team) within 24hours – following the *TCT Data Protection Policy*.
- I will not grant access to my school account or school devices entrusted to me to family or visitors or strangers
- If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: ____

Staff Signature: ________________________________

Date: _ _ /_ _ /_ _ _ _

Appendix 3: Online Safety Training Needs – Self-Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, Governors and visitors?	
Are you familiar with the school's Computing Charter for Pupils and the Parent/Carer Code of Conduct (in Home-School Diaries)?	
Do you regularly change your password for accessing the school's IT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	