SAFFRON VALLEY COLLEGIATE

BE READY, BE RESPECTFUL, BE SAFE

ONLINE SAFETY POLICY

Date of last review	**Summer Term 2026**
Review cycle	**Annual**
Policy due for review and approval by Local Governing Body	**Summer Term 2027**

Contents

Mission Statement 3
Equalities Statement 3
Introduction and Overview 4
Legislation and Guidance 5
Reviewing and Monitoring Online Safety 5
Roles and Responsibilities 6
Education and Curriculum 9
Expected Conduct and Incident Management 11
Managing IT and Communication System 14
Data Security: Management Information System Access and Data transfer 17
Equipment and Digital Content 18
APPENDIX 1 Acceptable Use Agreement 21
APPENDIX 2 Saffron Valley Collegiate Acceptable Use Policy (AUP) Agreement Form 24
APPENDIX 3 Key Stage 1: Acceptable Use Agreement 25
APPENDIX 4 Parents/Carers Acceptable Use Agreement 28
APPENDIX 5 Responding to Incidents: What do we do if? 31
APPENDIX 6 Device Loan Agreement 34
APPENDIX 7 Contract for Use of Equipment by Saffron Valley Collegiate (SVC) In Role of Employment 36
APPENDIX 8 GLOSSARY OF TERMS 37

Mission Statement

The Saffron Valley Collegiate seeks to provide a personalised educational experience that identifies and responds to the circumstances and needs of each individual child or young person. In doing so it enables them to progress academically and become successful learners through the re-engagement of the young person with education.

Equalities Statement

All who work at the Saffron Valley Collegiate are committed to the celebration of diversity, and the challenging of disadvantage and discrimination, in all of its forms.

These values are explicit to the ethos of the Saffron Valley Collegiate and implicit in all policies and practices.

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Ref: Keeping Children Safe in Education (DfE September 2025), Prevent Strategy – Implementation Policy, Behaviour for Learning Policy and Staff Code of Conduct.

Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Saffron Valley Collegiate (SVC) with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be 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	• Exposure to inappropriate content • Lifestyle websites promoting harmful behaviours • Hate content • Content validation: how to check authenticity and accuracy of online content
Contact	• Grooming, sexual exploitation, radicalisation etc. • Online bullying in all forms • Social or commercial identity theft, including passwords
Conduct	• Aggressive behaviours (bullying) • Intimidation/defamation of staff • Privacy issues, including disclosure of personal information • Digital footprint and online reputation • Health and well-being (amount of time spent online, gambling, body image) • Sexting (nudes/nude selfies): youth produced sexual imagery created to be erotic • Copyright (little care or consideration for intellection property and ownership
Commerce	• Online gambling • Inappropriate advertising • Phishing and/or financial scams

Scope

This policy applies to all members of the SVC 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 SVC.

Legislation and Guidance

This policy is based on the Department for Education'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
- Relationships and sex education
- 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' electronic devices where they believe there is a 'good reason' to do so

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils during induction.

Consultation:
The consultation in the production of this policy will involve:

- Local Governing Body (LGB)
- Teaching and support staff
- Pupils
- Parents/Carers
- ICT providers

Reviewing and Monitoring Online Safety

The Online Safety Policy is referenced within other school policies (e.g. Safeguarding, Early Help and Child Protection Policy, Behaviour for Learning Policy and PSHE Policy).

There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team (SLT) and approved by the Local Governing Body. All amendments to the school's Online Safety Policy will be disseminated to all members of staff and pupils.

Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• Must be adequately trained in off-line and online safeguarding, in line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance. • To lead a 'safeguarding' culture, ensuring online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision. • To take overall responsibility for data management and information security (SIRO) ensuring the school's provision follows best practice in information handling. • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGFL services. • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles. • To be aware of procedures to be followed in the event of a serious online safety incident. • Ensure suitable 'risk assessments' undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised. • To receive regular monitoring reports from the Online Safety Co-ordinator. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. Network Manager. • To ensure the Local Governing Body are regularly updated on the nature and effectiveness of the school's arrangements for online safety. • To ensure school website includes relevant information.
SVC Designated Safeguarding Lead/Online Safety Co-ordinator	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents. • Promote an awareness and commitment to online safety throughout the school community. • Ensure that online safety education is embedded within the curriculum. • Liaise with school technical staff where appropriate. • To communicate regularly with SLT, the nominated Safeguarding LGB Governor and the designated Online Safety Co-ordinator to discuss current issues, review incident logs and filtering/change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an online. safety incident • To ensure online safety incidents are logged as a safeguarding incident. • Facilitate training and advice for all staff. • Oversee any pupil surveys/pupil feedback on online safety issues. • Liaise with the Local Authority (LA) and relevant agencies. • Is regularly updated in online safety issues and legislation and be aware of the potential for serious child protection concerns. • To report online safety related issues that come to their attention, to the Headteacher. • To work with our IT services providers to manage the school's computer systems, through our arrangements with LGfL and Atomwide, ensuring: - School Password Policy is strictly adhered to - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)

Role	Key Responsibilities
	- access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis. • Keep up to date with the school's Online Safety Policy and any technical information in order to effectively carry out their online safety role and to inform and update others as relevant. • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Online Safety Co-ordinator/Headteacher. • To ensure appropriate backup procedures and disaster recovery plans are in place. • Reviewing and risk assessing new technologies and methodologies
Nominated Safeguarding LGB Governor	• To ensure that the school has in place policies and practices to keep the children and staff safe online. • To approve the Online Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents/carers and the wider community to become engaged in online safety activities. • The role of the nominated Online Safety LGB Link Governor will include regular reviews with the Designated Safeguarding Lead (DSL) and Online Safety Co-ordinator.
PSHE and Curriculum Wellbeing Co-ordinator	• To oversee the delivery of the online safety element of the PSHE and wider curriculum.
Data and Information (Asset Owners) Managers (IAOs)	• To ensure that the data they manage is accurate and up to date. • Ensure best practice in information management, i.e. have appropriate access controls in place, that data is used, transferred, and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner.
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant.
Teachers	• To embed online safety in the curriculum. • To supervise and guide pupils carefully when engaging in learning activities involving online technology (including, extended and extra-curricular school activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

Role	Key Responsibilities
All staff, volunteers and contractors.	• To read, understand, sign, and adhere to the school staff Acceptable Use Policy (AUP), and understand any updates. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the Online Safety Co-ordinator. • To maintain an awareness of current online safety issues and guidance e.g. through CPD. • To model safe, responsible, and professional behaviours in their own use of technology. • To ensure that conduct expectations are maintained when using IT and virtual environments. • To follow all school policies relating to the activity they are conducting and understand these may fall outside of the AUP (e.g. safeguarding). <u>Exit strategy</u> • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs, and passwords to allow devices to be reset, or meeting with Line Manager and Technician on the last day to log in and allow a factory reset.
Pupils	• Read, understand, sign, and adhere to the Pupil Acceptable Use Policy. • To understand the importance of reporting abuse, misuse, or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school. • To contribute to any 'pupil voice'/surveys that gathers information of their online experiences.
Parents/Carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/-ren. • To consult with the school if they have any concerns about their children's use of technology. • To support the school in promoting online safety and endorse the parents/carers' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent Groups	• Any external individual or organisation will sign an Acceptable Use Agreement prior to using technology or the Internet within school. • To support the school in promoting online safety. • To model safe, responsible, and positive behaviours in their own use of technology.

Education and Curriculum

Pupil Online Safety Curriculum

Saffron Valley Collegiate:

- has a clear, progressive online safety education programme as part of the PSHE and other curriculum areas. This covers a range of skills and behaviours appropriate to their age and experience.
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- will remind pupils about their responsibilities through the Pupil Acceptable Use Agreement(s).
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.
- ensures staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.
- ensure pupils only use school-approved systems and publish within appropriately secure/ age-appropriate environments.

Staff and Local Governing Body training

Saffron Valley Collegiate:

- makes regular training available to staff on online safety issues and the school's online safety education program.
- provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent/Carer awareness and training

Saffron Valley Collegiate:

- provides induction for parents/carers which includes online safety.
- runs a rolling programme of online safety advice, guidance, and training for parents/carers.

Cyber-bullying

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 1 person or group by another person or group, where the relationship involves an imbalance of power.

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. Teachers will discuss cyber-bullying with their tutor groups.

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, Local Governing Body, and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers 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 report the incident and provide the relevant material 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.

Examining Electronic Devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

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

- make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher.
- explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- seek the pupil's co-operation.

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 the staff member in conjunction with the Headteacher 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/carer 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.

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.

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

Expected Conduct and Incident Management

Expected Conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements.
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences.
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so.
- understand the importance of adopting good online safety practice when using digital technologies in and out of school.
- know and understand school policies on the use of mobile and hand-held devices including cameras.

Staff, volunteers, and contractors

- to know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form.
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions.
- everyone is 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 (i.e. the Local Authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, Internet Watch Foundation (IWF) in dealing with online safety issues.
- monitoring and reporting of online safety incidents take place and contribute to the developments in policy and practice in online safety within the school.
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, IWF and inform the LA.

Handling Incidents

- The school will take all reasonable precautions to ensure online safety.
- The school will seek to handle incidents of cyberbullying in accordance with the Behaviour for Learning Policy.
- Staff and pupils are given information about infringements in use and possible sanctions.
- The Headteacher, Online Safety Co-ordinator/SVC DSL act as first point of contact for any incident.
- Any suspected online risk or infringement is reported to the appropriate e-safety Lead that day.
- Any concern about staff misuse is always referred directly to the Headteacher unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the Local Authority's Designated Officer (LADO).

Handling a sexting/youth produced imagery/nude selfie incident

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken. Procedures should follow the REWIEW, RISK ASSESS, REFER model.

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  When assessing the risks the following should be considered:
  - *Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?*

- *Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?*
- *Are there any adults involved in the sharing of imagery?*
- *What is the impact on the pupils involved?*
- *Do the pupils involved have additional vulnerabilities?*
- *Does the young person understand consent?*
- *Has the young person taken part in this kind of activity before?*

- If a referral should be made to the police and/or children's social care.
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed.
- What further information is required to decide on the best response.
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services.
- Any relevant facts about the young people involved which would influence risk assessment.
- If there is a need to contact another school, college, setting or individual.
- Whether to contact parents/carers of the pupils involved - in most cases parents/carers should be involved.

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult.
2. There is reason to believe that a young person has been coerced, blackmailed, or groomed, or if there are concerns about their capacity to consent (e.g. owing to special educational needs).
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13.
5. You have reason to believe a pupil (or pupils) is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming.

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Managing IT and Communication System

Internet access, security (virus protection) and filtering

Saffron Valley Collegiate:

- informs all users that Internet/email use is monitored.
- has the educational filtered secure broadband connectivity through the LGfL.
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the Filtering Policy are logged and only available to staff with the approved 'web filtering management' status.
- uses USO user-level filtering where relevant.
- ensures network health through use of Sophos anti-virus software (from LGfL).
- uses DfE, LA, or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/ email to send 'protect-level' (sensitive personal) data over the Internet.
- uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.
- works in partnership with LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.
- uses specialised software to secure mobile and off-site devices, linked to user areas, for all staff and pupils.

Network Management (user access, backup)

Saffron Valley Collegiate:

- Uses individual, audited logins for all users - the LGfL USO system.
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services.
- Ensures the Systems Administrator/Network Manager is up to date with LGfL services and policies/requires the Technical Support Provider to be up to date with LGfL services and policies.
- Has daily back-up of school data (admin and curriculum).
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance.
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, Saffron Valley Collegiate:

- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network.
- All pupils have their own unique username and password which gives them access to the Internet and other services.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to log off when they have finished working or are leaving the computer unattended.
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection.

- Makes clear that pupils and staff are responsible for ensuring that any computer, laptop, or other device loaned to them by the school, is used primarily to support their schoolwork/ professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any corporate policies, e.g. Borough email or Intranet, finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed.
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems.
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems.
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data.
- Uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools.
- Ensures that all pupil-level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX).
- Our wireless network has been secured to industry standard Enterprise security level/ appropriate standards suitable for educational use.
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet Health and Safety standards.

Password Policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others. If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff to change their passwords into the MIS, LGfL USO admin site, every 90 days.
- We require staff using critical systems to use two factor authentication. Only staff with expressed authority are given these levels of access and only to the parts of the systems relevant to them.

E-mail

Saffron Valley Collegiate

- Provides staff with an email account for their professional use, London Staffmail, and makes clear personal email should be through a separate account.
- Uses anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk/ head@schoolname.la.sch.uk/ or class e-mail addresses.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Uses a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils

- We use LGfL, the pupil email system, which is intentionally 'anonymised' for pupil protection.

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff

- Staff can only use the LA or LGfL e-mail systems on the school system.
- Staff will use only LA or LGfL e-mail systems for professional purposes.
- Access in school to external personal e-mail accounts may be blocked.
- Never use their personal accounts for work related activity. If required to handle personal data off site they are provided with an encrypted laptop (and encrypted USB, if necessary and appropriate) or remote access to school servers.

School Website

- The Headteacher, supported by the Local Governing Body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- The school website complies with statutory DFE requirements.
- 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.
- Photographs published on the website 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.

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community.
- In school, pupils should only upload and publish within school approved 'Cloud' systems.

Social Networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications.
- All staff will adhere to the school's Social Media Policy.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers, or school staff.
- They should not be online friends with any pupil. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or LA and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report intimidation, misuse, or abuse through our online safety curriculum work.
- Are required to sign and follow our age-appropriate Pupil Acceptable Use Agreements.

Parents/Carers:

- Are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos, or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and pupil safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without the appropriate permission.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Data Security: Management Information System Access and Data transfer

Strategic and Operational Practices

At Saffron Valley Collegiate:

- The Headteacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are key contact(s) for key school information are (the Information Asset Owners). We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record.

Technical Solutions

- Safeguarding teams use secure a web platform to store safeguarding files.
- We require staff to log-out of systems when leaving their computer, and lock when not in use for shorter periods.
- We use the LGfL USO Auto Update, for creation of online user accounts for access to LGfL content and broadband services.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held, we get a certificate of secure deletion for any server that once contained personal data.
- We use secure file deletion software when hardware is decommissioned.

Equipment and Digital Content

Mobile Devices (mobile phones, tablets, and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, pupil and parents/carers or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft, or damage of personally owned mobile devices, other than those that are held in secure storage by school staff.
- At the KS3, KS4 North and South provisions: all pupil mobile devices are handed in to reception and returned to the pupil at the end of the school day. Mobile phones are stored securely.
- At the East provision: pupils hand in their mobile phones to the class teacher at the start of each lesson and are returned to the pupil at the end of the lesson. Mobile phones are stored securely.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher/SLT.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- No images or videos of other pupils should be taken on mobile devices without prior consent.
- Pupils should never take photos or film staff, using their personal devices.
- All visitors are requested to keep their phones on silent.
- The recording, taking, and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time if it is deemed necessary.
- The school reserves the right to search the content of a pupil's mobile device on school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence, or bullying.
- The Headteacher reserves the right to immediately contact the LADO should they have safeguarding concerns regarding the image contents/ appropriate use of a member of staff's mobile 'phone, camera, or other electronic device (refer to relevant parts of this policy). The LADO's guidance will be followed.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents/Carers are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break times.

Storage, Synching and Access – mobile devices

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the Network Manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the Network Manager.
- Exit process – when the device is returned the staff member must log in with their personal ID so that the device can be Factory Reset and cleared for reuse.

Pupils' use of personal devices

- The school accepts that there may be particular circumstances in which a parent/carer wishes for their child to have a mobile phone for their own safety.
- If a pupil breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.
- Pupils will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people, or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required, for instance for off-site activities where possible. If this is not possible staff will be given instructions of how to safeguard their private data should they need to use a personal device (see **'In an emergency'** below).
- Mobile phones and personally owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally owned devices will not be used during teaching periods unless permission has been granted by a member of the SLT in emergency circumstances.
- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- **In an emergency** where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident to the Headteacher/Designated Officer as soon as practicable.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Digital images and video

In this PRU:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the PRU, or as circumstances necessitate.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental/carer or pupil permission for its long-term, high-profile use.
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include LGB Governors, parents/carers or younger children as part of their learning.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

APPENDIX 1

Acceptable Use Agreement

All Staff, Volunteers and the Local Governing Body

Name of School	**Saffron Valley Collegiate**
AUA review Date	**Summer 2026**
Date of next Review	**Summer 2027**

What is an Acceptable Use Policy (AUP)?

We ask all children, young people and adults involved in the life of Saffron Valley Collegiate to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff, volunteers and the Local Governing Body have particular legal/professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

Where can I find out more?

All staff, volunteers and the Local Governing Body should read Saffron Valley Collegiate's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to Gareth Denton, Online Safety Co-Ordinator.

What am I agreeing to?

1. I have read and understood Saffron Valley Collegiate's full Online Safety Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.

2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult).

3. I understand the responsibilities listed for my role in the school's Online Safety Policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.

4. I understand that internet and device use in school, and use of school-owned devices, networks, and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.

5. I understand that I am a role model and will promote positive online safety and model safe, responsible, and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening, or violent comments about others, including the school staff, volunteers, Local Governing Body, contractors, pupils, or other parents/carers.

6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same.

7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety Policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.

8. I understand the importance of upholding my online reputation, that of the school and of the teaching profession), and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and in Saffron Valley Collegiate's social media policy/guidance.

9. I understand that school systems and users are protected by security and monitoring and filtering services, so my use of school devices (regardless of internet connection, time, or location) and networks/platforms/internet/other technologies, including encrypted content, may be monitored/captured/viewed by these systems and/or relevant/authorised staff members.

10. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform, or network, and will ensure I do not access, attempt to access, store, or share any data which I do not have express permission for. I will

protect my passwords/logins and other access, never share credentials, and immediately change passwords and notify [insert name/s] if I suspect a breach. I will not store school-related data on personal devices, storage, or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property, and copyright rules at all times.

11. I will use school devices and networks/internet/platforms/other technologies for school business and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring, will look after devices loaned to me, and will notify the school of "significant personal use" as defined by HM Revenue & Customs.

12. I will not support or promote extremist organisations, messages, or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download, or send material that is considered offensive or of an extremist nature by the school.

13. I understand and support the commitments made by pupils/students, parents/carers and fellow staff, Local Governing Body and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

14. I will follow the guidance in the Online Safety Policy for reporting incidents but also any concerns I might think are unimportant – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture, but only if I tell somebody. I have read the sections on handing incidents and concerns about a child in general, sexting, bullying, sexual violence and harassment, misuse of technology and social media.

15. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

APPENDIX 2:

Saffron Valley Collegiate Acceptable Use Policy (AUP) Agreement Form

All Staff, Volunteers, and Local Governing Body

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety/safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature…… Date……

Full Name…….. (printed)

Job Title/Role……

Authorised Signature (Headteacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature…… Date……

Full Name…… (printed)

SAFFRON VALLEY COLLEGIATE

BE READY, BE RESPECTFUL, BE SAFE

APPENDIX 3

Key Stage 1: Acceptable Use Agreement

I keep **SAFE online** because …

	✓
I **CHECK** it's OK to use a website / game / app.	
I **ASK** for help if I get lost online.	
I **THINK** before I click on things.	
I **KNOW** online people are really strangers.	
I am **RESPONSIBLE** so never share private information.	
I am **KIND** and polite online.	
I **TELL** a trusted adult if I am worried about anything.	
I do not take **PHOTOS** or **VIDEOS** of people without asking them first.	

My trusted adults are:

Mum
Dad
Teacher

My name:

Date signed:

If I do not act responsibly, I may be stopped from using the internet or IT equipment when there is no adult to help me.

SAFFRON VALLEY COLLEGIATE

BE READY, BE RESPECTFUL, BE SAFE

KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others.

- ***I am an online digital learner*** – I use the school's IT for schoolwork, homework and other activities approved by trusted adults.
- ***I am a secure online learner*** - I keep my logins and passwords secret.
- ***I am careful online*** - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.
- ***I am guarded online*** - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.
- ***I am cautious online*** - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.
- ***I am considerate online*** - I do not get involved with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these. I would never take photos or videos of other pupils without their permission, and **never** take photos or film staff, unless I have been instructed to do so with school equipment.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online.
- ***I am a creative digital learner online*** - I only edit or delete my own digital work and only use other people's work with their permission or where the work is shared through a Creative Commons licence.
- ***I am a researcher online*** - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.
- ***I communicate and collaborate online*** - with people I know and have met in real life or that a trusted adult has approved.
- ***I am SMART online*** - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.

I have read and understood this agreement.

I know who my trusted adults are and agree to the above.

If I do not act responsibly, I may be stopped from using the internet or IT equipment. I may also find that my devices may be removed from me until they can be collected by my parent/carer and/or I am banned from bringing them into school.

If I am involved in uploading photos or videos without permission, I will be asked to remove any offending material.

If I do not comply, SVC may consider involving the Police.

SAFFRON VALLEY COLLEGIATE

BE READY, BE RESPECTFUL, BE SAFE

KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others.

- ***I am an online digital learner*** – I use the school's IT for schoolwork, homework and other activities approved by trusted adults.
- ***I am a secure online learner*** - I keep my logins and passwords secret.
- ***I am careful online*** - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.
- ***I am guarded online*** - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.
- ***I am cautious online*** - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.
- ***I am considerate online*** - I do not get involved with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these. I would never take photos or videos of other pupils without their permission, and **never** take photos or film staff, unless I have been instructed to do so with school equipment.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online.
- ***I am a creative digital learner online*** - I only edit or delete my own digital work and only use other people's work with their permission or where the work is shared through a Creative Commons licence.
- ***I am a researcher online*** - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.
- ***I communicate and collaborate online*** - with people I know and have met in real life or that a trusted adult has approved.
- ***I am SMART online*** - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.

I have read and understood this agreement.

I know who my trusted adults are and agree to the above.

If I do not act responsibly, I may be stopped from using the internet or IT equipment. I may also find that my devices may be removed from me until they can be collected by my parent/carer and/or I am banned from bringing them into school.

If I am involved in uploading photos or videos without permission, I will be asked to remove any offending material.

If I do not comply, SVC may consider involving the Police.

SAFFRON VALLEY COLLEGIATE

BE READY, BE RESPECTFUL, BE SAFE

APPENDIX 4

Parents/Carers Acceptable Use Agreement

As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my son/daughter access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment (GSuite)
- IT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

The use of digital images and videos

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your son/daughter.

Saffron Valley Collegiate rules for any external use of digital images are:

- **If the pupil is named, we avoid using their photograph.**
- **If their photograph is used, we avoid naming the pupil.**

When showcasing examples of pupils' work, we only use their first names, rather than their full names. Only images of pupils in suitable dress are used. Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity, e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent/carer.
- Your child's image being used for presentation purposes around the school, e.g. in class or wider school wall displays or PowerPoint© presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools, or educators, e.g. within a DVD or a document sharing good practice, in our school prospectus or on our school website.
- In rare events, your child's picture could appear in the media, e.g. if a television crew or newspaper photographer attends an event. In this case you would be informed in advance of the visit and provided with an opportunity to withdraw your consent.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission.
I understand the school has a clear policy on "the use of digital images and video" and I support this.

The use of social networking and online media

This school asks its whole community to promote this common approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos, or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude, or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, homophobic, sexist, or defamatory.** This is online bullying and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs, and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. (All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP process for reporting abuse:
thinkuknow.co.uk/parents/

I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I will not take and then share online, photographs, videos etc., about other children (or staff) at school events, without permission.

I will support the school by promoting safe and responsible use of the Internet, online services, and digital technology at home. I will inform the school if I have any concerns.

I understand that if my son/daughter does not act responsibly they may be barred from using the internet/IT equipment.

My son/daughter's name: _____

Parent/Carer signature: _____

Date: _____

APPENDIX 5

Responding to Incidents: What do we do if?

This document is to be used as guidance. The list of responses is not exhaustive.

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the Headteacher/e-Safety Officer and decide whether to inform parents/carers of any children who viewed the site.
3. Inform Octavo IT and ensure the site is filtered (LGfL schools report to: **Atomwide via the LGFL Helpdesk**).

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Refer to the acceptable use policy that was signed by the child and apply agreed sanctions.
2. Notify the parents/carers of the child.
3. Inform the Octavo IT and ensure the site is filtered if need be.

An inappropriate website is accessed <u>intentionally</u> by a staff member.

1. Ensure all evidence is stored and logged.
2. Refer to the Acceptable Use and Staffing Policy that was signed by the staff member and apply disciplinary procedure.
3. Notify the Local Governing Body.
4. Inform Octavo IT and ensure the site is filtered if need be.
5. In an extreme case where the material is of an illegal nature:
   - Contact the local police, HR and LADO and follow their advice.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you – do not view the misuse alone.
2. Report the misuse immediately to the Headteacher (or named proxy) and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the Headteacher should then:
   - Remove the device to a secure place.
   - Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Contact HR and LADO and follow their advice.
   - Take appropriate disciplinary action (undertaken by Headteacher).
   - Inform the Local Governing Body of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police and follow their advice.
   - If requested, to remove the device to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either in or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to any relevant policies including Online Safety, Anti-bullying, and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents/carers of all the children involved.
6. Consider delivering a parent/carer workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection, LGFL)

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform Local Authority and other agencies (child protection, Local Governing Body, etc).

The school may wish to consider delivering a parent/carer workshop for the school community

You are concerned that a child's safety is at risk because you suspect that someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child.

1. Report to and discuss with the named Child Protection Officer in school and contact parents/ carers.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement of police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent/carer workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child.

1. Report to and discuss with the named Child Protection Officer in school and contact parents/ carers.
2. Advise the child and parents/carers on appropriate games and content. You may want to use LGFL template letters to inform all or targeted parents/carers.
3. If the game is played within school environment, ensure that the technical team block access to the game.
4. Consider the involvement of social services and child protection agencies.
5. Consider delivering a parent/carer workshop for the school community.

You are aware of social network posts and pages created by parents/carers about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Contact the poster or page creator and discuss the issues in person.
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact Local Governing Body.

4. Consider delivering a parent/carer workshop for the school community.

All of the above incidences must be reported immediately to the Headteacher and Online-Safety Officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

SAFFRON VALLEY COLLEGIATE

BE READY, BE RESPECTFUL, BE SAFE

APPENDIX 6
Device Loan Agreement

You are being provided with this device to support your learning. To make this work you need to commit to this agreement – signing this form means you have agreed to abide by the conditions below.

Refer also to the Acceptable Use Agreement that you signed on starting at the PRU.

Pupil's name:	
Item:	
Serial Number:	
Asset Register Number:	
Condition:	
Value:	
Date:	

As a learner I will:

- Look after the device very carefully all of the time.
- Always use the proper bag to carry the device and not overfill it with other items that could damage the device or the bag.
- Take care to keep the device as secure as possible when transporting it and never leave it unattended or visible in a car or other vehicle.
- Make sure it is not damaged by any careless or malicious behaviour by myself or my friends.
- Not decorate or change the case of the device in any way (this includes applying stickers and any sort of graffiti).
- Not use the device for any illegal and/or antisocial purpose or try to access any inappropriate internet sites or chat rooms.
- Take reasonable precautions to prevent the introduction of viruses e.g. not use the free CD/ DVDs given away with magazines; I will keep my USB stick virus free by only using it in the PRU's computers; the PRU will ensure the anti-virus software is up to date.

As a parent/carer I will:

- Ensure that our child understands how to care for and protect their device.
- Report any loss or damage (including accidental damage) promptly.
- Report any faults in hardware or software promptly.
- Ensure that the device is returned when the pupil leaves the PRU/when requested.
- Make sure the device is not used for any illegal and/or antisocial purpose, including access to inappropriate internet sites and chat rooms.
- Ensure that the PRU is promptly informed of any change of home location of the device (e.g. change of family address or different living arrangements).

Additional important information for families regarding the loan of a laptop:

- The device remains the property of Saffron Valley Collegiate (SVC), even when it is in your home. This also applies to any software or accessories issued.
- If the device is stolen you must immediately contact the police and get a crime reference number. You should then contact us (0203 252 2020) to report the loss.
- Failure to take reasonable care or to abide by the conditions listed in this document may result in the device being reclaimed.
- **SVC will consider asking for payment to cover repairs or replacement in the event of proven intentional damage.**

Student's Agreement – I agree to abide by these terms in the use of the device.

Name: _____

Signed: _____

Date: _____

Parent/Carer's Agreement – I agree to my child having the use of the device on these terms and understand that I may be held responsible for its use.

Name: _____

Signed: _____

Date: _____

Device Return

Date: _____

Name of staff member witnessing return: _____

APPENDIX 7

Contract for Use of Equipment by Saffron Valley Collegiate (SVC) In Role of Employment

Refer also to the Acceptable Use Agreement signed on starting at the SVC.

Staff member's name:	
Item:	
Serial Number:	
Asset Register Number:	
Condition:	
Value:	
Date:	

(Laptops): I understand that the laptop is encrypted for safeguarding of the asset and will not store the unlock key together with the laptop.

I understand that if my work involves keeping confidential data this will only be stored on an encrypted memory stick. No data will be stored on the hard drive.

I understand that this item belongs to SVC and is on loan to me during my employment or until the item is obsolete and will subsequently be written off in accordance with policy and procedures.

If the item goes missing during this period, I will be liable to replace the item at full value or, after a period of time, at a reduced value subject to time lapsed.

If I decide to terminate my role with SVC the item will be returned without delay prior to the final day of my employment.

Signed (staff member): .....

Role: .....

Signed: .....
Astrid Searle, Business Manager, Authorising Officer

Device Return

Date: .....

Name of staff member witnessing return: .....

APPENDIX 8
GLOSSARY OF TERMS

- AUA: Acceptable Use Agreement – *signed by an individual to indicate they agree with the terms of use of the internet and related technology.*
- DfE: Department for Education.
- DSL: Designated Safeguarding Lead – individual with responsibility for safeguarding within the school.
- Filtering: the act of blocking pupil/staff access to inappropriate sites.
- LA: Local Authority
- LGfL: London Grid for Learning – SVC's technology provider.
- Sexting: Youth produced sexual imagery, nudes, nude selfies or N4N (Nudes for Nudes). Images generated by young people that are deliberately created and often intended to be erotic.
- USB: (Universal Serial Bus) or flash drive - computer port which can be used to transport data.