ONLINE SAFETY POLICY (INGFIELD MANOR SCHOOL)

Policy implemented:	October 2023
Last reviewed:	October 2023
Next review due:	October 2024

1. Summary

Online Safety is of utmost importance to us and thus our school aims to:

- Have robust processes in place to ensure the online safety of students, 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 mobile and smart technology (which we refer to as 'mobile phones')
- 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.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

How the school will respond to issues of misuse

- Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use .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 ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. 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.

2. Document Control

Initial purpose and scope of the new policy/procedure agreed by:	Chris Brown Divisional Director (Education)
Sponsor Technical review carried out:	Principal Infield School
Final Information Governance quality check carried out:	Group Head of Regulation & Compliance
Date implemented:	October 2023
Version Number:	1.1
Date of the next review:	October 2024
Department responsible:	Education Opps
Job Title of Lead Person:	Sponsor Chris Brown

In addition to this policy, local authorities and other commissioners may have their own policies, procedures and guidance which Services must comply with. These policies should complement this policy.

However, there may be additional requirements put in place by local authorities and other commissioners and these must be adhered to. Changes must not be made to Salutem's policies and procedures without corporate approval but, where needed, local procedures should be developed to accompany these.

EQUALITY AND DIVERSITY STATEMENT

The Salutem Group is committed to the fair treatment of all in line with the Equality Act 2010. An equality impact assessment has been completed on this policy to ensure that it can be implemented consistently regardless of any such factors and all will be treated with dignity and respect.

3. Contents

1. Summary 1
2. Document Control 3
3. Contents 4
4. Definitions 5
5. Principles 5
6. Areas of Governance 6
7. Areas of Responsibility 7
8. Learning and Development 9
9. Associated Documents 9
10. Useful Links 17
11. References 17
12. Version Control 17

This policy must be brought to the attention of all employees.
The controlled version of this policy and its associated documents are available on the eLFY bookshelf.
Printed or downloaded copies are uncontrolled and may not be up to date.

4. Definitions

Online Safety- refers to the practice of protecting oneself and others from potential risks and threats while using the internet. This includes measures to secure personal information, avoid cyberbullying, and prevent exposure to harmful content or online scams.

Cyberbullying- Cyberbullying 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.

5. Principles

Educating students about online safety

Students will be taught about online safety as part of the curriculum. Online safety is delivered as part of the ICT and PSHE curriculum. Considering the cognitive needs of our student group, online safety lessons are differentiated to meet their individual needs. The following key definitions are for guidance only and individual student levels are recorded on teachers MTPs.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. At Ingfield Manor School, filtering and monitoring of online activity is carried out by firewall and monitoring software. 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.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This topic is also discussed at key tutor group times including assemblies, Safer Internet Day, PSHE lessons, and other subjects where appropriate.
All staff and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).
The school also sends updates to parents on online safety which may include information on cyber-bullying. The DSL will report any incident relating to cyber-bullying 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.

Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use. We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. School owned devices are not permitted to be sent home unless agreed the principal, DSL and IT manager and an individualized agreement is in place to support this.

Students using mobile devices in school

Students may bring mobile devices into school (for the purpose of use on transportation), but are not permitted to use them during school hours: Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2). Students are able to bring mobile phones on site but are expected to hand them to staff at the beginning of the day where they are stored in a secure locker. Mobile devices are then returned to students at the end of the school day - see the school's uniform and personal possession policy.

Staff using work devices outside school

Individual staff members are responsible for:

- Not sharing the device among family or friends
- Making sure the device locked if they step away from it
- Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices should not be used for any activity which could be deemed as illegal or harmful to others. If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

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, e-bulletins and staff meetings). All staff will receive training on filtering and monitoring at least once each academic year. 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 and proprietors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training

6. Areas of Governance

This policy has been written with expert contribution from appropriate stakeholders. The Information Governance Team will monitor, reflect on and gain organisational learning from the implementation of

this policy. This policy will be reviewed and updated two years from implementation unless legal changes demand a more timely amendment.

The application of this policy and its associated documents is mandatory for all services staff, volunteers, agency staff and all other Salutem representatives. Staff understanding of this policy and associated documents will be assured through training, assessment of competency and supervision.

Staff understanding of this policy will be assured through training and the delivery of awareness raising workshops as deemed necessary by SLT. The people we support will be involved in the review to ensure it captures the important issues for them.

7. Areas of Responsibility

Governance Responsibility

All staff and governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT 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 teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and students with special educational needs and/or disabilities (SEND). We recognise that our student group will need a more personalised and contextualised approach to meet their needs.

Principal Responsibility

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

The designated safeguarding lead Responsibility

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Manage and monitor all internal online safety issues and incidents in line with the school child protection policy.
- Ensuring that any internal online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately.
- Updating and delivering staff training on online safety as part of the school's internal safeguarding training. Monitoring that are completing their online 'online safety' training (appendix 4 contains a self-audit for staff on online safety training needs).
- Liaising with the school's IT manager.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports and/or audits on online safety in school to the principal.

The ICT Manager Responsibility

- 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 students 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 ICT 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 ICT systems on a regular 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 (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately.

All Staff and Volunteers Responsibility

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that students follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
  Ensuring that any incidents of cyber-bullying are dealt with appropriately
- 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'
- Child contact staff are responsible for physically monitoring the use and appropriateness of devices in class.
- Staff are responsible for ensuring that no personal devices from home are used within school hours.

Parents Responsibility

- 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 ICT systems and internet (appendices 1 and 2)
- Parents can seek further guidance on keeping children safe online from the following organizations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and Members of the Community

- Visitors and members of the community who use the school's ICT 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 3).

8. Learning and Development

Salutem is committed to ensuring that all staff are aware of what is expected of them so that everyone is appropriately supported. Staff should speak to their line manager in relation to their learning needs using supervision and through the appraisal process.

Include any relevant additional information about training plans, etc here.

9. Associated Documents

Appendix 1: Primary student acceptable use agreement (students and parents/carers)

ICT Acceptable Use Policy (EYFS & Primary Students)

Your device*, the software that runs on it, the internet and other bits of ICT equipment will play an important part of your life in school. We try to make the computers as safe as possible to protect you but you need to use them correctly and safely too.

These rules will help you do that. By signing this document you are agreeing to follow the rules at all times.

- I will use my device carefully.
- My device is for me, it should not be used by anyone else.

- I will only use the programs that are already on my device and not download any from the internet.
- I will not go on the internet unless I am with a member of staff.
- I will tell a member of staff if there is anything on my device I don't understand, am unhappy with or do not like.
- I will not tell anyone on the internet any personal details.
- I understand that, if I bring my mobile phone to school, it will be locked away during school hours and returned to me at the end of the day. If I use it during the evening in Acorns it must be with a member of staff present.
- I understand that my device may be checked.
- I understand that if I break the rules I may not be able to use my device, the network or the internet.

User Signature

I agree to abide by the Ingfield Manor School ICT Acceptable Use Policy Primary (June 2023)

Signature Date

Full Name (printed)

This form must be signed by the pupil or a parent/carer or an IMS staff member as appropriate

*device in this context means any computer, laptop, VOCA or tablet that has been provided by Ingfield Manor School.

Appendix 2: Secondary student acceptable use agreement (students and parents/carers)

ICT Acceptable Use Policy (Secondary Students)

Your device*, the software that runs on it, the internet and other ICT equipment will play an important part of your life in school. We try to make the computers as safe as possible to protect you but you need to use them correctly and safely too.

This policy is designed to ensure that you are aware of your responsibilities when using any form of ICT. All students are expected to sign this policy and follow it at all times.

- I will treat my device and all other ICT related items with care and respect.
- I agree and accept that any device loaned to me by the school, is provided solely to support my communication and/or schoolwork, it should not be used by anyone else.
- I will only share my user login and password with my parents/carers, when not in school.
- I will only use software and memory sticks that have been provided by school.
- I will not access the internet unless I have been instructed to by a member of staff.
- I will not download anything from the internet unless instructed by a member of staff.
- I will tell a member of staff if there is anything on my device I don't understand, am unhappy with or do not like.
- I will not attempt to visit internet sites that may be considered inappropriate or search for inappropriate material.
- I will not access social networking sites, chat rooms or instant messaging sites in school, unless it is a curriculum related activity.
- I will only use my approved school email account at school.
- I will not open emails or attachments from people I do not know.
- I will inform a member of staff immediately if I receive an offensive email or an email from an unknown source.
- I will always be polite and sensible and be careful not to use language which could offend.
- I will not forward chain letters etc
- I will not reveal any personal information (eg address, phone numbers) about myself or others.
- I know that bullying in any form will not be tolerated.
- I will not arrange to meet anyone I do not know. I will report any request immediately to a member of staff.
- I understand that, if I bring my mobile phone to school, it will be locked away during school hours and returned to me at the end of the day.
- I understand that mobile phones, Skype etc are for use during evening activities only unless being used as part of a lesson.
- I will not use my mobile phone, Skype unless it is with the direct supervision of a member of staff.

- I understand that my device/laptop may be checked and internet sites I visit monitored.
- I understand that if I break the rules I may be denied access to my device/laptop, the network and the internet and my equipment may be confiscated.

_____

User Signature

I agree to abide by the Ingfield Manor School ICT Acceptable Use Policy Secondary (June 2023)

Signature Date

Full Name (printed)

This form must be signed by the pupil or a parent/carer or an IMS staff member as appropriate

*device in this context means any computer, laptop, VOCA or tablet that has been provided by Ingfield Manor School.

Appendix 3: Sixth Form student acceptable use agreement (students and parents/carers)

ICT Acceptable Use Policy (Sixth Form)

Your device*, the software that runs on it, the internet and other bits of ICT equipment will play an important part of your life in school. We try to make the computers as safe as possible to protect you but you need to use them correctly and safely too.

This policy is designed to ensure that you are aware of your responsibilities when using any form of ICT. All students are expected to sign this policy and follow it at all times.

- I will treat my device and all other ICT related items with care and respect.
- I agree and accept that any device loaned to me by the school, is provided solely to support my communication and/or schoolwork, it should not be used by anyone else.
- I will only share my user login and password with my parents/carers when not in school. I will not attempt to access a computer using someone else's login and I will not allow other people to use mine.
- I will only use software and memory sticks that have been provided by school.
- I will not intentionally change the settings on the device/laptop.
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.

- During school hours I will not access the internet unless I have been instructed by a member of staff.
- I will not download anything from the internet unless instructed by a member of staff.
- I will only take pictures or videos of people if I have the person's permission.
- I will only post pictures or videos on the internet if they are appropriate and I have the person's permission.
- I will not attempt to visit internet sites that may be considered inappropriate or search for inappropriate material.
- I will only use my approved school email account at school.
- I will not open emails or attachments from people I do not know.
- I will inform a member of staff immediately if I receive an offensive email or an email from an unknown source.
- I will always be polite and sensible and be careful not to use language which could offend.
- I will not forward chain letters etc.
- I understand that mobile phones, social media etc are for use during evening activities only unless being used as part of a lesson. I will not access them during school hours.
- I will let the Shift Lead know which social media sites I wish to access in the evenings and will not try to access others.

- I will only contact people through social media that have been agreed by my parents/carers. If necessary, I will set up a separate account for use in school.
- I will give the school access to my accounts if requested.
- I will not reveal any personal information (eg address, phone numbers) about myself or others.
- I will not arrange to meet anyone I do not know. I will report any request to meet up immediately to a member of staff.
- I know that bullying in any form will not be tolerated.
- I will tell a member of staff if there is anything on my device/laptop I don't understand, am unhappy with or do not like.
- I understand that my computer may be checked and internet sites I visit monitored.
- I understand that if I break the rules I may be denied access to my device/laptop, the network and the internet and my equipment may be confiscated.

_____

User Signature

I agree to abide by the Ingfield Manor School ICT Acceptable Use Policy Sixth Form (June 2023)

Signature Date

Full Name (printed)

This form must be signed by the pupil or a parent/carer or an IMS staff member as appropriate

Appendix 4: Over 18's student acceptable use agreement (students and parents/carers)

ICT Acceptable Use Policy (Over 18's)

Your device*, the software that runs on it, the internet and other bits of ICT equipment will play an important part of your life in school. We try to make the computers as safe as possible to protect you but you need to use them correctly and safely too.

This policy is designed to ensure that you are aware of your responsibilities when using any form of ICT. All students are expected to sign this policy and follow it at all times.

- I will treat my device and all other ICT related items with care and respect.
- I agree and accept that any device loaned to me by the school, is provided solely to support my communication and/or schoolwork, it should not be used by anyone else.
- I will only share my user login and password with my parents/carers when not in school. I will not attempt to access a computer using someone else's login and I will not allow other people to use mine.
- I will only use software and memory sticks that have been provided by school.
- I will not intentionally change the settings on the device. I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- During school hours I will not access the internet unless I have been instructed by a member of staff.
- I will not download anything from the internet unless instructed by a member of staff.
- I will only take pictures or videos of people if I have the person's permission.
- I will only post pictures or videos on the internet if they are appropriate and I have the person's permission.
- I will not attempt to visit internet sites that may be considered inappropriate or search for inappropriate material.
- I will only use my approved school email account when in lessons.
- I will not open emails or attachments from people I do not know.
- I will inform a member of staff immediately if I receive an offensive email or an email from an unknown source.
- I will always be polite and sensible and be careful not to use language which could offend.
- I will not forward chain letters etc.
- I understand that mobile phones, social media etc are for use during evening activities only unless being used as part of a lesson. I will not access them during school hours.
- I will give the school access to my accounts if requested.
- I will not reveal any personal information (eg address, phone numbers) about myself or others.
- I will not arrange to meet anyone I do not know. I will report any request to meet up immediately to a member of staff.
- I know that bullying in any form will not be tolerated.

- I will tell a member of staff if there is anything on my device I don't understand, am unhappy with or do not like.
- I understand that my computer may be checked and internet sites I visit monitored.
- I understand that if I break the rules I may be denied access to my device, the network and the internet and my equipment may be confiscated.

_____

User Signature

I agree to abide by the Ingfield Manor School ICT Acceptable Use Policy Over 18's (June 2023)

Signature Date

Full Name (printed)

This form must be signed by the pupil or a parent/carer or an IMS staff member as appropriate

*device in this context means any computer, laptop, VOCA or tablet that has been provided by Ingfield Manor School.

10. Useful Links

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Complaints procedure
- ICT and internet acceptable use policy
- Uniform and personal possessions policy

https://www.ingfieldmanorschool.co.uk/policies/

https://www.gov.uk/government/publications/the-prevent-duty-safeguarding-learners-vulnerable-to-radicalisation

11. References

- Education Act 2011
- Equality Act 2010
- Education and Inspections Act 2006

12. Version Control

This is a controlled document. As a controlled document, any printed copies of this document, or saved onto local or network drives should be actively monitored to ensure the latest version is always available.

Version Number	Date	Status	Changes
V1.0	October 2023	Draft	New policy