St. Jérôme
Church of England
Bilingual School

Online Safety Policy

September 2024

Executive Headteacher: _____
(Reverend D Norris)

Chair of the Governing Body: _____
(Ian Fernandes)

Date: _____

Date of review: September 2025

Contents

2.1 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including 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, anti-Semitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2.1 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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
- 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.

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

2.1 3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Marie Noelle Stacey.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's 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, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's 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 Online Safety Co-ordinator in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with DSLs, Online Safety Co-ordinator and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- 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 logged and dealt with appropriately in line with the school behaviour policy
- Ensuring updated staff training on online safety is delivered(appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Reviewing regular reports on online safety in school from the Online Safety Co-ordinator

This list is not intended to be exhaustive.

3.4 The Online Safety Co-ordinator

The Online Safety Co-ordinator is responsible for:

- Ensuring an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Monitoring the school's ICT systems on a monthly basis
- Ensuring that access is blocked 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 in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL and Online Safety Co-ordinator 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 in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 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.

2.1 4. Educating pupils about online safety

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

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

In Key Stage 1, pupils will be taught to:

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

Pupils in Key Stage 2 will be taught to:

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

By the end of primary school, pupils will know:

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

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

2.1 5. 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.

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

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

2.1 6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

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

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

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

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

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 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 cooperation

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

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

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

If inappropriate material is found on the device, it is up to 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 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 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 Intethernet 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
- Our behaviour policy

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

2.1 7. Acceptable use of the internet in school

All staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

2.1 8. Pupils using mobile devices in school

Student use of and retention of mobile phones and other internet-enabled devices are not allowed in school. Students who need to carry mobile phones to and from school will leave their devices (turned-off) at the office as soon as they arrive at school.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

2.1 9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

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

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 must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Online Safety Co-ordinator.

2.1 10. 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 teaching about using ICT safely. 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 ICT usage agreement and staff code of conduct. 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.

2.1 11. Training

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

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

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

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

Training will also help staff:

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

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They – and the Online Safety Co-ordinator - will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

2.1 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Online Safety Co-ordinator. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

2.1 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use agreement
- Teaching of using ICT safely

Appendix 1a: acceptable use agreement (staff, volunteers and visitors)

Saint Jérôme Church of England Bilingual School

ICT User Agreement
Staff, Volunteers and Governors

Headteacher_____

Chair of the Governing Body_____

Date: March 2023

All the employees of Saint Jérôme Church of England Bilingual School (the School) have the opportunity to use the School's extensive ICT resources. To qualify to use these resources all staff need to read and agree to the terms of this ICT user agreement.

The School strongly supports the use of ICT and every effort will be made to provide reliable resources to all users, however inappropriate and/or illegal use of any ICT resource is strictly prohibited.

Please take some time to read the following document carefully. Listed are the provisions of the agreement, if any user violates this agreement access to ICT resources will be denied and the user may be subject to disciplinary action.

Acceptable Use: All Users

1. Personal Responsibility

As a representative of the School you will accept personal responsibility for reporting misuse of ICT resources to a member of the School SLT. Misuse may come in many forms, but is commonly viewed as any information sent, received or viewed that indicates or suggests pornography, unethical or illegal activities, racism, sexism, inappropriate language or any use of which may be likely to cause offence.

2. Network Etiquette and Privacy

You are expected to abide by the generally accepted rules of network etiquette. These rules include but are not limited to the following:

- BE POLITE. Never send or encourage others to send messages with abusive material.
- USE APPROPRIATE LANGUAGE. Remember that you are a representative of The School. Never use inappropriate language. Discussion of Illegal activities is strictly prohibited.
- PRIVACY. Do not reveal any personal information to anyone especially the home address or personal details of yourself or any others.
- E-MAIL. Electronic Mail (E-Mail) is not guaranteed to be private. Messages are screened for inappropriate material, and although in most cases this takes place automatically, your message may be individually screened. Messages supporting illegal or inappropriate activities may be reported to the relevant authorities.
- DISRUPTIONS. Do not use the ICT resources in a way that could be disruptive to others.
- OTHER CONSIDERATIONS. Remember that humour and satire are very easily misinterpreted. Respect the rights and beliefs of others.

3. Services

The School makes no guarantees of any kind whether expressed or implied for the ICT service that is provided. The School denies any responsibility for the validity or accuracy of any information obtained by its internet services. We do not recommend or endorse the storage of data outside of our network. If information is stored locally, for example on a laptops, the individual user is responsible for ensuring that their data is securely backed up.

4. Security

Security on our ICT services is very important. If you discover a security problem, please inform a member of the IT Department via support@crossover.solutions as soon as possible. Never demonstrate this problem to another user. All use of the ICT systems must be under your own username and password. Anyone found to be sharing accounts and passwords may have their access blocked. Any user identified as a security risk may have their access blocked and be subject to a disciplinary action.

5. Vandalism

Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or any other networks that are connected to the system. This includes but is not limited to, uploading and/or creation of computer viruses, the wilful damage of computer hardware and deletion of data.

6. Electronic Mail & Messaging

An official email address will be provided to all staff members. This is the only email account which should be used to conduct work. Users are expected to use these services in a responsible manner. The sending of any emails that breach the terms of the ICT User Agreement will result in disciplinary actions. Bulk sending of email without prior permission (spamming) is also forbidden.

7. Monitoring

All users email and system accounts have been provided to them by the School and should not be considered personal accounts. They are loaned to the indivdual for duration of the time at the School in order to undertake specific activities. The School reserves the right to monitor activity, using both automated systems (scanning for file types, file content) and manually.

Where there is sufficient reason to do so appropriate individuals will be granted access to the accounts.

8. Disciplinary Consequences

- If the rules of the Acceptable Usage Policy are broken users will have their computer privileges removed, this includes logon abilities, access to email and access to the internet. Depending on the severity of the issue one or more of the above restrictions may be implemented.
- If a Staff member breaches the Acceptable Usage Policy any incident will be reported to HR and the Senior Leadership Team for further action.

Acceptable Use: Workforce, Governors and Volunteers.

The use of ICT resources must be in support of the role perform for the School. You are personally responsible for this provision at all times when you use any of the ICT resources.

By using any The School IT equipment after reading this ICT user Agreement means that you understand and accept these terms and conditions listed below Any breach of these conditions may lead to severe consequences!

I. I will only use the school's email (gmail)/ Internet / Intranet / and any related technologies for professional purposes or for uses deemed acceptable by the Headteacher or Governors.

II. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

III. My passwords will be "strong" in nature, and include capitals, lower case, number, and symbol and be of least 8 characters long. If I suspect it has been compromised, then I will change it immediately.

IV. I will ensure that I am the only one who uses my user Account and understand that anything undertaken while I am logged in, I will be held responsible for.

V. I will not autosave my password or log in details for any the School systems, as this negates the effectiveness of the password.

VI. I will lock my computer screen whenever I leave it unattended.

VII. I will ensure that all electronic communications are compatible with my professional role.

VIII. If I receive a suspicious email, I will report it before clicking on any links, downloading any attachments or entering my user details. When I report it, I will not forward the email but send a screen shot.

IX. My personal social media accounts will not show a direct link with the School, and I understand that whatever I post can be seen, therefore if I am identifiable content will be of a professional nature.

X. I will only use the approved, secure e-mail system(s) for any School business and will always check if I should be CC'ing Bcc'ing recipients and that the correct email address, and attachment has been selected.

XI. I will ensure that personal data is kept secure and is used appropriately, whether in the office, or when working remotely. Personal data should be stored on the google drive.

XII. I will transfer personal data by email securely e.g. using egress, or password protecting it. The password will be sent in a sperate email.

XIII. I understand that anything I write in an email or document about an identifiable person can be requested via a Subject Access Request and read by that indivdual. Therefore, would not write anything that I would not want that person to read, could bring the organisation in disrepute or is counter to the staff code of conduct.

XIV. I will not install any hardware or software without the permission of the IT Department.

XV. I will consider if the communications I send breach confidentiality or the Data Protection Act, by asking "should the recipient view this information".

XVI. I understand that I can cause a Data Protection breach by destroying or corrupting data and all data should be held in line with The School's data retention schedule.

XVII. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

XVIII. I will support the School's approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the organisation or its community' onto my own social media platforms.

XIX. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Senior Leadership Team.

XX. I will respect copyright and intellectual property rights.

XXI. I will ensure that my online activity, both in work and outside work, will not bring The School my professional reputation, or that of others, into disrepute.

XXII. I will not use the School's ICT systems for any commercial activities, such as work for a for-profit organisation.

Print Name:	Sign:
Date:	

Appendix 1b: acceptable use agreement (governors)

Saint Jérôme Church of England Bilingual School

ICT User Guidance for Governors

Headteacher_____

Chair of the Governing Body_____

Date: March 2023

Governors should familiarise themselves with the following school policies:

- Acceptable use and e-safety
- Data Protection

- Breach Management

Governors should be mindful of the 7 principles of UK GDPR and the Data Protection Act:

1. Keep information secure
2. Only store data for as long as you need or are legally required to do so
3. Only use the data required to do your job
4. Only use data for the purpose specified
5. Ensure accuracy of data
6. Handle data transparently
7. Accountability – you need to justify why you have acted as you have

Practical guidance for governors:

- Governing Body documentation is stored electronically on the shared portal or securely in hard copy in line with the School's Document Retention Policy. Personal copies of documents should be retained in line with the school data retention schedule.

- Any information downloaded from the shared portal onto a personal device should be deleted upon the completion of the task, including from the temporary internet files.

- School email addresses should be used for school business. This prevents subject access requests to personal email accounts and facilitates compliance with any email retention period. Please note, that this email address can be monitored by appropriate individuals if there is due cause.

- When discussing business over emails, individuals should be identified only as case reference numbers or initials.

- Email conversations should be professional at all times. Email messages are required to be disclosed in legal proceedings or in response to Subject Access requests from individuals under the Data Protection Act 2018 in the same way as paper documents.
- Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, therefore do not write anything you would not want to read by others

- When using personal devices please ensure that the device has anti-virus in place has been updated to limit potential vulnerabilities.

- Your passwords should be "strong" in nature, and include capitals, lower case, number, and symbol and be of least 8 characters long. If you suspect it has been compromised, then it must change immediately.
  Do not autosave your password or log in details for any school systems, as this negates the effectiveness of the password.

- We appreciate that others may use the personal devices you access the system with however please ensure that you are the only person who can access your user Account and

that you understand that anything undertaken while you are logged in, will be considered done by you.

- Governors must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information, or the data of multiple individuals should be encrypted so that the information is only accessible by the intended recipient.
- If Governors receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

- The school via the School Business Manager, should be informed of any confirmed or potential data breaches without undue delay to allow it to react and mitigate the impact.

User Declaration and Signature

I agree to abide by the ICT Policy and guidance

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)

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

Signature: Date:

Name: Signature:

Appendix 2: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident