



# John Grant School

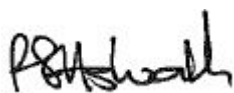
'Working together, to be the best that we can be.'

## Online Safety Policy

### Policy Consultation & Review

This policy is posted on our school website and is available on request from the school office. John Grant School is part of 'Trust Norfolk SEN' and is committed to all of the standards and procedures maintained by the Local Authority.

This policy will be reviewed in full by the Governing Body on an annual basis. This policy was last reviewed and agreed by the Governing Body in September 2021. It is due for review on September 2022

Signature  Headteacher Date: 08.09.21

Signature  Vice Chair of Governors Date: 08.09.21

## Contents

1. Aims .....	2
2. Legislation and guidance .....	2
3. Roles and responsibilities .....	3
4. Educating pupils about online safety.....	4
5. Educating parents about online safety .....	5
6. Cyber-bullying.....	5
7. Acceptable use of the internet in school! .....	6
8. Pupils using mobile devices in school .....	6
9. Staff using work devices outside school .....	6
10. How the school will respond to issues of misuse.....	6
11. Training .....	?
12. Monitoring arrangements .....	7
13. Links with other policies .....	7
Appendix 1: acceptable use agreement (pupils and parents/carers) .....	8
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) .....	9
Appendix 3: online safety training needs - self-audit for staff .....	10

### 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

### 2. 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 [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department’s guidance on [protecting children from radicalisation](#).

Co-ordinator: DSL

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](#).

### **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).

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 2)

#### **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 designated safeguarding leads (DSL) are set out in our child protection and safeguarding policy.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Network Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged using a pink form and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or

governing board This list is not intended to be exhaustive.

#### **3.4 The Network Manager**

The Network Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 4) 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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.

### **3.6 Parents**

Parents are expected to:

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

Ensure that if their child is considered capable, has read, understood and agreed to the terms on acceptable

use of the school's ICT systems and internet (appendix 1)

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

websites:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/490001/Social\\_Media\\_Guidance\\_UKCCIS\\_Final\\_18122015.pdf.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf.pdf)

<https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

<https://www.bbc.co.uk/cbeebies/grownups/article-internet-use-and-safety>

<https://www.ceop.police.uk/safety-centre/>

There is a link on the home page of the school website to CEOP for members of the school community who would like more advice about internet safety or who wishes to report a matter regarding internet safety.

## **4. Educating pupils about online safety**

Pupils will be taught about online safety as part of the Computing curriculum and as part of the PSHE curriculum. Students will be taught using both discrete and integrated lessons whilst taking into account the very special needs of our students. Full details can be found in the Computing Progression of Skills document.

By the end of their time at John Grant School, it is hoped that the majority of students will be able 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

While some students will be able to:

- Use technology, the internet and social media safely, respectfully and responsibly, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

The school may invite speakers to talk to pupils about this.

## **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. This policy will also be shared with parents.

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.

## **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 endeavor to ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will provide information so 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 during PSHE and computing lessons.

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 safeguarding 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**

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete

Co-ordinator: DSL



inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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

## **7. Acceptable use of the internet in school**

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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 and 2.

## **8. Pupils using mobile devices in school**

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

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.

## **9. Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

Work devices must be used solely for work activities.

#### **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 the safeguarding policy. 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.

## **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).

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

## **12. Monitoring arrangements**

The DSLS logs behaviour and safeguarding issues related to online safety. These are reported using the pink form.

This policy will be reviewed bi-annually by the Subject Leader. At every review, the policy will be shared with the governing board.

## **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

## Appendix 1: Acceptable Use Agreement

### Pupil Acceptable Use Agreement

So that I can stay safe on the internet, I agree to the following:

- I will keep my passwords secret
- I will only look at my own work and files
- I will only use the computer for things a staff member has told me to
- I will make sure that all the messages I send are polite
- I will tell a member of staff if I see something that makes me feel scared or uncomfortable on the screen
- I will not reply to any nasty message or anything that makes me feel uncomfortable. I will show a member of staff
- I will not tell people about myself online (I will not tell them my name, birthday, mobile phone number, anything about my home, family, pets and school)
- In school, I will only use my school email
- I will only email people I know or who a member of staff says it is okay to email
- I will never agree to phone, message or meet a stranger
- I will not put photographs of myself online
- I will not upload images or video of other people without their permission
- Where work is copyrighted (including music, videos and images,) I will not either download or share with others
- I will not use the system for gaming, gambling, shopping, or uploading videos or music
- I know that members of staff can check what I do online and that if I break the rules I might not be allowed to use a computer in school

Signed (student) \_\_\_\_\_

Signed (parent / carer) \_\_\_\_\_

Date: \_\_\_\_\_

\_\_\_\_\_

## **Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)**

### **Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors**

**Name of staff member/governor/volunteer/visitor:**

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and Network Manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

Co-ordinator: DSL

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

**Signed (staff member/governor/volunteer/visitor):**

**Date:**

**Appendix 3: online safety training needs – self-audit for staff**

Online safety training needs audit	
<b>Name of staff member/volunteer:</b>	<b>Date:</b>
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school’s acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school’s ICT systems?	
Are you familiar with the school’s approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	



