**Foveran School**



**Online safety Policy**

**Internet Safety Policy**

**Scope of the Policy**

6

This policy applies to all members of the school community (including staff, children / young people, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school

Schools need to be aware that incidents of cyber-bullying, or other e-safety incidents covered by this policy may take place outside of the school, between children and young people who attend the school or between any members of the school community, including staff. The school and the education authority, in partnership with parents needs to decide how to deal with such incidents and make this clear in the policy. This will link closely with positive relationships and behaviour policy and anti-bullying policies. The policy should make clear how the school will involve parents in relation to such incidents.

**Roles and Responsibilities**

7

**Headteacher**

The Headteacher should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

* sharing of personal data;
* access to illegal / inappropriate materials;
* inappropriate on-line contact with adults / strangers;
* potential or actual incidents of grooming;
* cyber-bullying;
* Inappropriate sharing of images, for example through mobile phones.

T**he Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the class teacher.

T**he Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff**

The Headteacher are responsible for ensuring that the E-Safety staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

**Teaching and Support Staff**

are responsible for ensuring that:

**• they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;**

**• they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP);**

**• they report any suspected misuse or problem to the *Headteacher* for investigation and action;**

**• all digital communications with children/young people / parents / carers should be on a professional level** *and only carried out using official school systems;*

• e-safety issues are embedded in all aspects of the curriculum and other activities;

• children / young people understand and follow the e-safety and acceptable use policies;

• children / young people have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

• teachers monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;

*• in lessons where internet use is pre-planned children/young people should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*

Children / young people:

* **are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy for children/young people;**
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. They need to **un**derstand the need to protect themselves and respect others when participating in social networks;
* will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying;
* should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school;
* should demonstrate an understanding of digital citizenship and how it links to their roles and responsibilities within the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to work closely in partnership with parents on these issues through *parents’ evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

**•** digital and video images taken at school events;

• access to parents’ sections of the website / VLE and on-line student / pupil records;

• their children’s personal devices in the school (where this is allowed).

11

Policy Statements

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Some parents may have extensive knowledge and expertise in this area and be able to support the school.

The school will therefore seek to provide information and awareness to parents and carers through:

*• curriculum activities;*

*• letters, newsletters, web site, VLE;*

*• parents / carers evenings / sessions;*

*• high profile events / campaigns for example Safer Internet Day;*

*• reference to the relevant web sites / publications for example* [*www.swgfl.org.uk*](http://www.swgfl.org.uk)[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>

Use of digital and video images

**•** When using digital images, staff should inform and educate children / young people about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites, or sending inappropriate /intimate digital images which then may be shared further;

•in accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (such activity for personal use is exempt under the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children / young people in the digital / video images;

•staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purpose;

•care should be taken when taking digital / video images that children / young people are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;

•children / young people must not take, use, share, publish or distribute images of others without their permission;

•photographs published on the website, or elsewhere that include children / young people will be selected carefully and will comply with good practice guidance on the use of such images;

•children/Young People’s full names will not be used anywhere on a website or blog, particularly in association with photographs;

•written permission from parents or carers will be obtained before photographs of children / young people are published on the school website

•learners’ work can only be published with the permission of the children / young people and parents or carers.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

|  |  |  |
| --- | --- | --- |
| 18User Actions | Unacceptable | Unacceptable and illegal |
| **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:**  | **Child sexual abuse images The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978** |  | X |
| **Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.** |  | X |
| **Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008** |  | X |
| **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986**  |  | X |
| **pornography** | X  |  |
| **promotion of any kind of discrimination** <http://www.equalityhumanrights.com/advice-and-guidance/education-providers-schools-guidance/> | X  |  |
| **threatening behaviour, including promotion of physical violence or mental harm** [Offensive Behaviour at Football and Threatening Communications (Scotland) Act 2012](http://www.scottish.parliament.uk/parliamentarybusiness/CurrentCommittees/31384.aspx) | X  |  |
| **threatening behaviour, including promotion of physical violence or mental harm** | X  |  |
| **any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute** | X  |  |
| **Using school systems to run a private business** | X |  |
| **Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school** | X |  |
| **Infringing copyright** | X |  |
| **Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)** | X |  |
| **Creating or propagating computer viruses or other harmful files** | X |  |

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

**If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.**

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of concern **all steps in this procedure should be followed:**

* Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported;
* Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure;
* It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection);
* Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below);
* Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following;
* Internal response or discipline procedures;
* Involvement by Local Authority or national / local organisation (as relevant);
* Police involvement and/or action;
* **If content being reviewed includes images of Child Abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:**
* incidents of ‘grooming’ behaviour;
* the sending of obscene materials to a child;
* adult material which potentially breaches the Obscene Publications Act;
* criminally racist material;
* other criminal conduct, activity or materials;
* **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Responses to internal incidents

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

22

23

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to protect myself and respect others and ensure there is no risk to the safety and security of the ICT systems and other users.

**For my own personal safety:**

* I understand that the *school* will monitor my use of the ICT systems, email and other digital communications.
* I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
* I will be aware that I cannot trust people when I am communicating on-line because they may not be who they say they are.
* I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc. )
* If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
* I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
* **I understand that everyone has equal rights to use technology as a resource and:**
* I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
* I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
* I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission from a member of staff to do so.

25

**I will act as I expect others to act toward me:**

* I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
* I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will not take or distribute images of anyone without their permission.

I understand that being a responsible digital citizen means that I have the same standards of relationships and behaviour in an online community as I do in the school community.

**I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:**

* I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
* I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.
* I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
* I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
* I will only use chat and social networking sites with permission and at the times that are allowed.

**When using the internet for research or recreation, I recognise that:**

* I should ensure that I have permission to use the original work of others in my own work
* Where work is protected by copyright, I will not try to download copies (including music and videos)
* When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

**I understand that I am responsible for my actions, both in and out of school:**

* I understand that the school will respond to incidents of inappropriate behaviour out with school as set out in relevant school policies..
* I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be held accountable to the school. This may mean loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *children / young people* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that children / young people receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

• I understand that the school will monitor my use of the ICT systems, email and other digital communications.

• I understand that the rules set out in this agreement also apply to use of school ICT systems (for example laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school

• I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

• I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

28

* I understand the concept of digital citizenship and will model good citizenship online and reinforce messages linking policies and standards on positive behaviour in school and in online communities such as social networks.

I will be professional in my communications and actions when using school ICT systems:

• I will not access, copy, remove or otherwise alter any other user’s files, without their express permission.

• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school’s policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (for example on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

• I will only use chat and social networking sites in school in accordance with the school’s policies.

• I will only communicate with children / young people and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with children / young people and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)

• I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

• When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• I will ensure that my data is regularly backed up, in accordance with relevant school policies.

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

• I will not disable or cause any damage to school equipment, or the equipment belonging to others.

• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

• I understand that data protection policy requires that any staff or child / young person data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

• I will ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

• I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Education Authority and/or Governors / Directors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

• Erase or amend data or programs without authority;

• Obtain unauthorised access to a computer;

• “Eavesdrop” on a computer;

• Make unauthorised use of computer time or facilities;

• Maliciously corrupt or erase data or programs;

• Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

• Fairly and lawfully processed.

• Processed for limited purposes.

• Adequate, relevant and not excessive.

• Accurate.

• Not kept longer than necessary.

• Processed in accordance with the data subject’s rights.

• Secure.

• Not transferred to other countries without adequate protection.

Freedom of Information (Scotland) Act 2000

The Freedom of Information (Scotland) Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information (Scotland) Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Regulation of Investigatory Powers Act (Scotland) 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

• Establish the facts;

• Ascertain compliance with regulatory or self-regulatory practices or procedures;

• Demonstrate standards, which are or ought to be achieved by persons using the system;

• Investigate or detect unauthorised use of the communications system;

• Prevent or detect crime or in the interests of national security;

• Ensure the effective operation of the system.

• Monitoring but not recording is also permissible in order to:

• Ascertain whether the communication is business or personal;

• Protect or support help line staff.

• The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

• Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

• Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

50

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Sexual Offences (Scotland) Act 2009

The Sexual Offences (Scotland) Act defines consent and allows one party to withdraw it at any stage, whether they initially gave consent or not .The act also gives a legal recognition of male rape.

The Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005

This legislation introduces a new offence of sexual grooming of a person under 16; It also introduces Risk of Sexual Harm Orders (RSHOs) which are designed to protect children from those who display inappropriate behaviour towards them; It introduces a new offence of paying for the sexual services of a person under 18; It introduces new offences of causing, inciting, controlling, arranging or facilitating the provision of sexual services by children or child pornography; It amends current legislation criminalising the taking, possessing and distribution of indecent images of children so that it applies to images of people under 18 rather than only to images of those under 16;

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

• The right to a fair trial

• The right to respect for private and family life, home and correspondence

• Freedom of thought, conscience and religion

• Freedom of expression

• Freedom of assembly

• Prohibition of discrimination

• The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

[**Offensive Behaviour at Football and Threatening Communications (Scotland) Act 2012**](http://www.scottish.parliament.uk/parliamentarybusiness/CurrentCommittees/31384.aspx)

Focuses on behaviour at Football matches, but also **criminalises the communication of threats of serious violence and threats intended to incite religious hatred, whether sent through the post or posted on the internet.** The Act will only criminalise behaviour likely to lead to public disorder which expresses or incites hatred, is threatening or is otherwise offensive to a reasonable person.

**Equalities Act 2010**

UK Government legislation applicable to Scotland. Reforms and harmonises equality law and restates previous legislation relating to discrimination and harassment related to seven personal characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex, and sexual orientation.

# The Head Teacher at Foveran School welcomes feedback on this document.

**Contact:**

Foveran School

Main Road

Foveran

Ellon

Aberdeenshire

AB41 6AZ

Tel: 01358 281115

E mail: Jamie.ferguson@aberdeenshire.gov.uk