ICT and Communications Systems Policy and Declaration

Agreed by Governors on 20/03/2017

Statutory policy: Yes, required by Governors

Signed by Chair of Governors: Sally Birkbeck

Frequency of review period: Annually Document History

Document History:

Date	Description
01/05/12	Agreed by Governors
May 2012	Summary Statement signed by staff
February 2013	Summary Statement signed by staff
Ongoing	Summary Statement signed by visitors, interviews etc.
12/05/14	Agreed by Governors
11/05/15	Agreed by Governors
21/03/16	Agreed by Governors
20/03/17	Agreed by Governors

ADAPTED FROM PACT HR POLICY AUGUST 2013

1. Policy Statement

This policy is to be read in conjunction with the school's Mobile Phone, Data Protection, Safeguarding and Preventing Extremism and Radicalisation Policies and applies to all staff, governors, regular visitors to the school, including students, and candidates on recruitment. It is to be issued to all staff, governors and regular visitors on its adoption by the Governing Body and when new staff, governors and regular visitors are provided with access to the ICT network on any school provided and compatible device e.g. Laptop, tablet, mobile phone. The policy will be made available to candidates on recruitment interviews when they arrive in school. This policy has been written in support of the obligations of both the Prevent Duty and the DFE's statutory guidance on Keeping Children Safe In Education.

The Governing Body recognises the use of its ICT and communications facilities as an important resource for teaching, learning and personal development and as an essential aid to business efficiency. It actively encourages staff to take full advantage of the potential for ICT and communications systems to enhance development in all areas of the curriculum and school administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate material.

All employees, supply agency staff, consultants, volunteers and contractors are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the declaration, retaining a copy themselves and returning the other to the school office.

Policy Coverage

This policy covers the use by staff, governors, regular visitors to the school, including students, and candidates on recruitment of all ICT and communications systems/equipment provided for work purposes and equipment which is on loan to staff by the school for their personal or study use. Examples of such systems/equipment include:

- laptop, desktop computers**,** tablets such as iPads
- ICT network facilities e.g. shared file areas
- personal digital organisers and handheld computers
- mobile phones and phone/computing hybrid devices
- USB drives and other physical storage devices
- Cloud based storage systems
- Image data capture and storage devices including cameras, camera phones and video equipment
- E-mail and other secure and approved cloud or offsite based data sharing and storage systems e.g. secure shared area via the school website.

This list is not exhaustive.

2. The use of school ICT and Communications Facilities

Use of School ICT Equipment

The Governing Body expects all use of ICT equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times. **All users must uphold the school's Code of Confidentiality.**

Individuals who use the school's ICT and communications systems:

- must use them responsibly
- must use them safely in accordance with the highest level of safeguarding procedures
- must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries
- must comply with the schools 90 day password change policy which ensures a minimum 7 character password with at least1 capital letter and 1 number
- must report any known breach of password confidentiality to the Head teacher or nominated ICT Co-ordinator as soon as possible
- must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems
- must report to the Head teacher any vulnerabilities affecting child protection in the school's ICT and communications systems
- must not install software on the school's equipment, including freeware and shareware, unless authorised by the school's ICT support technician
- must comply with any ICT security procedures governing the use of systems in the school, including anti-virus and data protection measures
- must ensure that it is used in compliance with this policy
- must not attempt to remove any pre-installed software from school issued ICT equipment e.g. anti-virus, e-safe software etc.
- must not tamper with or make changes in any way to school issued ICT equipment.

Any equipment provided to a member of staff should not be used by any person who has not seen and signed a copy of this ICT & communication systems policy. Any misuse of the equipment by unauthorised users will be the responsibility of the staff member to whom that piece of equipment has been assigned and must be reported to the head teacher immediately.

Prohibited Usage of Email and Internet and Communications Systems

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any breaches of this policy or operation of the school's equipment outside statutory legal compliance may be grounds for disciplinary action being taken.

The following uses of the school's ICT system are prohibited and may amount to gross misconduct and could result in dismissal:

- to make, to gain access to, or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it
- to make, to gain access to and/or for the publication and distribution of material promoting homophobia or racial or religious hatred or radicalisation in relation to any subject, opinion or belief
- for the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, culture, religious belief, disability, age or sexual orientation or gender reassignment
- for the publication and/or distribution of libelous statements or material which defames or degrades others. This applies across any platform of ICT including social media, email or online communication method not mentioned here.
- for the publication of material that defames, denigrates or brings into disrepute the school and/or its staff and pupils
- for the publication and distribution of any personal data without authorisation, consent or justification
- where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination
- to participate in on-line gambling
- where the use infringes copyright law
- where the use infringes Data Protection
- to gain unauthorised access to internal or external computer systems (commonly known as hacking)
- to create or deliberately distribute ICT or communications systems "malware", including viruses, worms, etc.
- to record or monitor telephone or email communications without the express approval of the Governing Body (or the Chair of Governors). In no case will such recording or monitoring be permitted unless it has been established for that such action is in full compliance with all relevant legislation and regulations (see Regulation of Investigatory Powers Act 2000, below) Regulation of Investigatory Powers Act 2000.
- to enable or assist others to breach the Governors' expectations as set out in this policy

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

- for participation in "chain" e-mail correspondence (including forwarding hoax virus warnings)
- in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade unions)
- to access ICT facilities by using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity.
- the use of a non-school issued, non-encrypted USB memory stick

- although it is very appropriate to take photographs and use a range of media to record a curriculum activity, to celebrate school life and to evidence assessment and progress, providing we have permission to do so from parents, staff MUST NOT use their personal equipment, e.g. mobile phone, camera, IPAD etc to take edit or store images (still or moving) of pupils

SECURITY AND SAFEGUARDING

Security

Staff must not write down any passwords to school systems or equipment. The safest solution is for an individual to save login information to their personal school area in a folder which is not immediately obvious. School login information must not be saved to portable ICT equipment such as iPads or Phones as these can easily be lost or stolen.

All use of the school computers is logged and sites visited recorded and monitored. The school ICT technician will actively monitor staff compliance with this policy through a variety of technologies including:

- Smoothwall firewall protection and logs
- E-safe forensic software
- Anti-virus software
- Windows server level reporting and event logs
- Exchange email management portal
- Unique individual computer history and logs
- Egress email encryption reporting

This list is not exhaustive.

During annual ICT equipment inventory checks all loaned equipment such as laptops, iPads and school provided mobile phones will be subjected to a routine sampling exercise where the ICT technician will perform hardware/software and internet usage tests. This will be a random sampling exercise, but exists to ensure harder to monitor usage such as external home usage is monitored and more secure. This is because systems such as E-safe forensic and Smoothwall are not included when working external to the school building. These checks will be recorded by the school ICT technician annually. Any violations to school ICT policy may be subject to disciplinary procedures.

School provided mobile phone usage is also monitored externally by O2 and Millgate Communications. The school Business Support Team receive a monthly online report detailing numbers dialled and texted. Data usage is also monitored and a report is generated to show the monthly analysis by each individual phone.

Remote Access

When working from home staff must ensure they are using the school implemented remote access services to access the school network. The use of encrypted memory sticks can be used as a contingency if for any reason staff cannot access the school system remotely.

Virtual Private Network (VPN)

This is an encrypted and very secure form of remote access for staff who have been assigned a school laptop. School equipment installed with this type of VPN remote access must always prioritise this technology when working externally to the schools internet connection and network. This will ensure all access on school laptops both internal and external to the school is secure and monitored through the schools safeguarding and security filtering systems. If access to this VPN technology is ignored and not used at any time external to the schools network/internet then this would be deemed as being in violation of this policy and disciplinary action may follow.

Safeguarding - e-Safe

An Online safety Forensic Monitoring ICT system is in operation at Delius. This system is used to ensure the highest standards of safeguarding for the children, staff, governors and the school community at Delius are in place. This system provides:

- weekly summary reports detailing information of transgressing behaviour busive behaviour)
- daily reports within 24 hours of an incident occurring which may require priority intervention
- immediate escalations by telephone of a serious incident which may be a threat of violence or serious self-harm etc. All reports sent via email will be sent directly to senior Delius Named Persons for Child Protection, i.e. the Head Teacher, Deputy Head Teacher or Senior Assistant Head Teacher. If the report concerns the Head Teacher it will be sent to Bradford Local Authority*.*
- for incidents which are considered to be life threatening or potentially illegal, a confidential phone call at the earliest possible opportunity to explain the details of the incident and guidance on the *next steps will be made by e-safe to the school.*

Email encryption

Delius uses Egress, an email encryption system set up to work with school-provided email accounts. Egress should always be used when sending personal information or information deemed as confidential via email correspondence both internally and externally to the school.

Use of Equipment for Taking Photographs

Photographs of pupils should only be taken on school equipment for school use. This may include pupils from visiting schools or on trips and at events held at school providing permission has been obtained from the member of staff in charge of the visiting pupils. This applies to the following school equipment:

- School provided iPads
- School provided cameras including video cameras

Images should be uploaded to the school's shared areas and deleted from the mobile device as soon as possible. This is to reduce the risk of mobile devices being lost or stolen whilst containing images of Delius pupils.

Staff must not use their personal mobile phones, cameras or any other image capturing technology to take pictures of pupils whilst on Delius school business.

Staff should not use school iPads and cameras to take pictures of their own children, or of other children outside of Delius school business.

Social Networking

- **Access to any public social networking sites are prohibited at any time on school provided ICT equipment. This is to eliminate the risk of unauthorised images of Delius pupils or any school data from being uploaded accidently. This is also to eliminate the risk of Delius pupils falling victim to the viewing of inappropriate content held on these sites.**
- Staff should not communicate with pupils through personal/private email accounts, social networking sites, even on educational matters, but should use school email and only other forms of correspondence sanctioned by school.
- Staff should be circumspect in their use of social networking sites on personal ICT equipment and must not discuss business or school issues on their personal social networking accounts.
- All social networking sites are restricted through the school's internet access.
- We encourage positive comments and "likes" on the school Facebook page, this is essential for building an online community and promoting the school to a wider online audience. However please be mindful of the image you're presenting through your own personal Facebook account when "liking" and commenting on the school Facebook page. It is important to realise when commenting and "liking" through Facebook that your own profile picture and potentially your entire profile is then linked to the schools page. This must be appropriate for a school.

Note: The restrictions within this policy apply to the use of phones, e-mails, text messaging, internet chatrooms, blogs and personal websites (including personal entries on Facebook etc) inclusive of any future technologies. This list is not exhaustive.

PERSONAL USE OF SCHOOL ICT EQUIPMENT

In addition to their normal access to the school's ICT and communications systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment and email during their own time subject to such use:

- not depriving pupils of the use of the equipment;
- not interfering with the proper performance of the staff member's duties; and
- not being for abusive purposes
- If ICT equipment has VPN access installed, all personal usage must also be accessed through this secure and monitored connection.

Personal Email

Staff are permitted to access their personal email accounts on school iPads and laptops, however this must not be within school working hours or anywhere close

to where a Delius pupil might be at risk of accessing the account. Staff must log out of personal email accounts immediately when finished and must not click to save login information for next use.

Access to any public social networking sites are prohibited at any time on school provided ICT equipment.

Regulation of Investigatory Powers Act 2000

Ancillary to their provision ICT facilities the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer (including e-mails) or telephonic communications systems and will do so where there are grounds for suspecting that such facilities are being, or may have been, misused.

In the event of offensive material being found on a school computer which may have been placed there by a member of staff, remove the computer from use and put it in a secure place and seek immediate advice from your HR Business Partner.

3. Legal issues relevant to the use of ICT and communications equipment

Computer Misuse Act 1990

This was introduced as a means of prosecuting individuals who commit some form of computer crime. Hacking, eavesdropping, deliberate virus attacks are covered. Unauthorised access to a computer is the most likely offence within the Council. Only use machines/systems which you are authorised to use.

Data Protection Act 1998

Individuals have rights about personal data recorded on computer and in manual files. Don't put personal data in the subject line of emails; be careful about including it in the body of the text. An individual can request access to his personal data and this includes email. There are regulations about direct marketing via email.

Copyright, Design & Patents Act 1988

It is an offence to copy software without the author's permission. Downloading application software without permission or forwarding programs in attachments may put you in breach of this act. Some Internet sites will not let you copy material you find there Take care.

The Defamation Act 1996

Facts concerning individuals or organisations must be accurate and verifiable views or opinions must not portray their subjects in a way that could damage their reputation. This applies to internal as well as external email. Organisations in the UK have lost court cases where internal email systems were used to defame other organisations and heavy fines were imposed.

Sex Discrimination Act 1975 Race Relations Act 1976 Disability Discrimination Act 1995 Protection from Harassment Act 1997

Accessing or distributing material which may cause offence to individuals or damage the Council's reputation may lead to a prosecution under these Acts. The fact that it is electronic does not prevent action.

Human Rights Act 1998

The present Government's commitment to incorporating the European Convention on Human Rights into domestic law has led to the introduction of the Human Rights Act 1998. Under this Act a UK citizen can assert their Convention rights through the national courts without having to take their cases to the European Court of Human Rights.

Obscene Publications Act 1959

All computer material is subject to the conditions of this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.

'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending, offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act. The publisher would appear to be the originator or poster of the item. The Council is the originator of the Bradford Internet & Intranet sites, or the Governing Body in the case of Voluntary Aided and Foundation schools.

Telecommunications Act 1984

The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under section 43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

Protection of Children Act 1978 Criminal Justice Act 1988

These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

PART 1: to be retained by staff/governor/volunteer/visitor (etc)

This declaration refers to the Governing Body's policy and guidance on the use the school's ICT and communications systems and confirms that you have been provided with a copy and that you have agreed to follow it.

All employees, supply agency staff, consultants and contractors are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the following declaration.

Declaration

You should sign two copies of this document; this copy is to be retained by you. The second copy (below) is to be detached and placed your personal file.

I confirm that I have been provided with a copy of the school's policy on the use of the school's ICT and communications systems. I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies even if I am working from home on school equipment or networks.

Signed: ..... Name: ..... Date:……

✂----------

PART 2: to be detached and kept by school

This declaration refers to the Governing Body's policy and guidance on the use the school's ICT and communications systems and confirms that you have been provided with a copy and that you have agreed to follow it.

All employees, supply agency staff, consultants and contractors are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the following declaration.

Declaration

You should sign two copies of this document; this copy is to be retained on your personal file.

I confirm that I have been provided with a copy of the school's policy on the use of the school's ICT and communications systems. I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies even if I am working from home on school equipment or networks.

Signed: ..... Name: ..... Date: ……