GDPR – TRAINING FOR SCHOOL GOVERNORS

MONDAY 4TH JUNE2018

OUTCOMES

- INCREASE KNOWLEDGE OF GDPR LEGISLATION
- UNDERSTAND HOW GDPR WILL AFFECT OUR SCHOOL
- UNDERSTAND GDPR JARGON
- UNDERSTAND THE ROLE OF GOVERNORS/ TRUSTEES

KEY TERMS

- GDPR – GENERAL DATA PROTECTION REFORM
- ICO – INFORMATION COMMISSIONER'S OFFICE


1998

DATA GENERATION

- 1992 -100GB OF DATA GENERATED DAILY
- 1997 -100GB OF DATA GENERATED **HOURLY**
- 2002 -100GB OF DATA GENERATED **PER SECOND**
- 2013-28,875GB OF DATA GENERATED PER SECOND
- 2018 -50,000 GB PER SECOND

ESTIMATED DATA PER MINUTE TODAY

- 216,000 INSTAGRAM POSTS
- 204,000,000 EMAILS
- 12 HOURS OF FOOTAGE IS UPLOADED TO YOUTUBE
- 277,000 TWEETS ARE POSTED

GENERAL DATA PROTECTION REGULATION (GDPR)

EUROPEAN WIDE LEGISLATION.

IMPLEMENTATION ON 25TH MAY 2018 – FIXED DATE.

CONTRACTUAL, STATUTORY AND REGULATORY OBLIGATIONS.

SANCTIONS – FOR SCHOOLS AND INDIVIDUALS.

BREACHES OF THE REGULATIONS – DAMAGE TO REPUTATIONS.

DATA PROTECTION OFFICER APPOINTMENT – JOHN WALKER

DATA AND DATA SUBJECTS – ARTICLE 4 (1)

DATA IS:

- ANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON

A DATA SUBJECT IS:

- AN IDENTIFIABLE PERSON, ONE WHO CAN BE IDENTIFIED, DIRECTLY OR INDIRECTLY, IN PARTICULAR BY REFERENCE TO AN IDENTIFIER SUCH AS A NAME, IDENTIFICATION NUMBER, LOCATION DATA (ADDRESS), INTERNET ADDRESS OR ONLINE IDENTIFIER.
- OR TO ONE OR MORE FACTORS SPECIFIC TO PHYSICAL, GENETIC, MENTAL, ECONOMIC, CULTURAL OR SOCIAL IDENTITY OF A PERSON.

SENSITIVE DATA – ARTICLE 9 (1)

FOLLOWING ARE CONSIDERED SENSITIVE:

- RACIAL OR ETHNIC ORIGIN INFORMATION
- POLITICAL OPINIONS
- RELIGIOUS OR PHILOSOPHICAL BELIEFS
- TRADE UNION MEMBERSHIP
- HEALTH OR SEXUAL LIFE INFORMATION
- GENETIC INFORMATION
- BIOMETRIC DATA

DATA PROCESSING – ARTICLE 4 (2)

PROCESSING "MEANS ANY OPERATION OR SET OF OPERATIONS PERFORMED UPON PERSONAL DATA OR SETS..

- WHETHER OR NOT BY AUTOMATED MEANS, SUCH AS COLLECTION, RECORDING, ORGANISATION, STRUCTURING, STORAGE, ADAPTATION
- OR ALTERATION, RETRIEVAL, CONSULTATION
- ERASURE OR DESTRUCTION
- OR OTHERWISE MAKING AVAILABLE

DATA PROCESSORS – ARTICLE 4 (7)

- WE ARE **ALL** DATA PROCESSORS.

DATA CONTROLLER – ARTICLE 4 (7)

- 'CONTROLLER' MEANS THE NATURAL OR LEGAL PERSON, PUBLIC AUTHORITY, AGENCY OR ANY OTHER BODY, WHICH ALONE OR JOINTLY WITH OTHERS, DETERMINES THE PURPOSES AND MEANS OF PROCESSING OF PERSONAL DATA.
- THE DATA CONTROLLER IS THE BOARD OF TRUSTEES FOR THE MULTI-ACADEMY TRUST.

RESPONSIBILITIES OF DATA CONTROLLERS

- ENSURE COMPLIANCE
- STAFF UNDERSTAND THEIR OBLIGATIONS
- ENSURE POLICIES AND PROCEDURES ARE FIT FOR PURPOSE
- HAVE CONFIDENCE THAT PROCEDURES AND POLICY IS BEING IMPLEMENTED
- UNDERSTAND WHAT ACTIONS TO TAKE IN RESPONSE TO A BREACH
- SUPPORT THE SCHOOL TO ENSURE COMPLIANCE

THE SIX PRIVACY PRINCIPLES OF GDPR

- **LAWFULNESS, FAIRNESS AND TRANSPARENCY**
- YOU HAVE TO HAVE A LAWFUL REASON TO COLLECT THE DATA. PEOPLE HAVE A RIGHT TO KNOW HOW THE DATA WILL BE USED, AND IT SHOULD IN A WAY THEY DON'T EXPECT.
- **PURPOSE LIMITATIONS**
- DATA CAN ONLY BE USED FOR THE REASON IT WAS COLLECTED IN THE FIRST PLACE. PRIVACY NOTICES TELL PEOPLE HOW IT WILL BE USED.
- **DATA MINIMISATION**
- IT IS ONLY PERMISSIBLE TO COLLECT DATA THAT IS NECESSARY TO PERFORM A FUNCTION. YOU SHOULDN'T COLLECT OR ACCESS AND PROCESS DATA SIMPLY BECAUSE IT IS THERE.
- **ACCURACY**
- IT IS IMPORTANT TO HAVE A PROCESS TO CHECK IF THE INFORMATION ON FILE IS STILL ACCURATE.
- **STORAGE LIMITATIONS**
- DATA SHOULD NOT BE KEPT FOR LONGER THAN IS NEEDED, A CLEAR RETENTION POLICY NEEDS TO BE IN PLACE AND APPLIED.
- **INTEGRITY AND CONFIDENTIALITY**
- DATA SHOULD BE KEPT SECURE, THIS APPLIES TO HARD COPY AND DIGITAL INFORMATION. KEEPING DATA SECURE IN THE CLASSROOM AND ANYTIME IT IS IN USE IN OUTSIDE SCHOOL MEETINGS IS CRITICAL. WHEN YOU HAVE DATA IN YOUR POSSESSION, YOU ARE RESPONSIBLE FOR THAT DATA.

RIGHTS FOR INDIVIDUALS

- RIGHT TO BE INFORMED – WHAT'S COLLECTED AND WHY?
- RIGHT OF ACCESS
- RIGHT TO RECTIFICATION
- RIGHT TO ERASURE
- RIGHT TO OBJECT - NO ANSWER IS **NOT** CONSENT

- THIS INFORMATION IS AVAILABLE THROUGH OUR PRIVACY NOTICES WHICH CAN BE VIEWED ON THE SCHOOL'S WEBSITE.

NEW PROVISIONS IN RESPECT OF CHILDREN

- **•PRIVACY NOTICES FOR CHILDREN**
- •WHERE SERVICES ARE OFFERED DIRECTLY TO A CHILD, YOU MUST ENSURE THAT YOUR PRIVACY NOTICE IS WRITTEN IN A CLEAR, PLAIN WAY THAT A CHILD WILL UNDERSTAND.
- **•ONLINE SERVICES OFFERED TO CHILDREN**
- •IF YOU OFFER AN ONLINE SERVICE TO CHILDREN, YOU MAY NEED TO OBTAIN CONSENT FROM A PARENT OR GUARDIAN TO PROCESS THE CHILD'S DATA.
- •THE GDPR STATES THAT, A CHILD UNDER THE AGE OF 16 CAN'T GIVE THAT CONSENT THEMSELVES AND SO MUST BE FROM A PERSON HOLDING 'PARENTAL RESPONSIBILITY'. IT WILL ALLOW MEMBER STATES TO PROVIDE FOR A LOWER AGE IN LAW, AS LONG AS IT IS NOT BELOW 13.
- •THE GDPR EMPHASISES THAT PROTECTION IS PARTICULARLY SIGNIFICANT WHERE CHILDREN'S PERSONAL INFORMATION IS USED FOR THE PURPOSES OF MARKETING AND CREATING ONLINE PROFILES.
- •PARENTAL/GUARDIAN CONSENT IS NOT REQUIRED WHERE THE PROCESSING IS RELATED TO PREVENTATIVE OR COUNSELLING SERVICES OFFERED DIRECTLY TO A CHILD.

SUBJECT ACCESS REQUESTS (SAR)

INDIVIDUALS

- HAVE THE RIGHT O KNOW WHAT AN ORGANISATION HOLDS ABOUT THEM.
- HAVE THE RIGHT TO SEE WHAT'S HELD ABOUT THEM.
- CAN ASK FOR MISTAKES TO BE REMEDIED OR DELETED

- PROCESS REQUIRED TO RECORD THE REQUEST AND VIEWING OF DATA.
- NO DATA CAN BE WITHHELD.
- COMPLIANCE MUST BE WITHIN ONE MONTH.

3RD PARTIES AND SUPPLIERS

- DATA CONTROLLER HAS THE RESPONSIBILITY TO ENSURE DATA PROTECTION PROCESSES ARE FOLLOWED.
- A SUITABLE CONTRACT MUST BE IN PLACE.
- PROCESSES MUST BE CLEARLY DEFINED.
- SUB-CONTACTING CAN ONLY TAKE PLACE WITH THE CONTROLLERS AGREEMENT.
- CONTROLLER MUST BE CONTACTED IN CASE OF A BREACH.
- THERE MUST BE AN AGREEMENT IN PLACE TO ASSIST THE CONTROLLER IN THE EVENT OF A BREACH.

WHEN THINGS GO WRONG

- SENDING EMAILS TO INCORRECT ADDRESSES.
- LOSING FILES AND INFORMATION.
- NOT LOCKING A COMPUTER.
- OTHERS SEEING INFORMATION THAT THEY SHOULDN'T.
- SENSITIVE DATA LEFT LYING AROUND.
- SHARING DATA IN ERROR OR DELIBERATELY.
- SHARING DATA WITHOUT LAWFUL REASON.

More

DATA SECURITY

- HARD COPIES – ON & OFF SITE
- EMAILS – SCHOOL SYSTEM AND INSTRUCTIONS
- 3RD PARTY SYSTEMS
- MEMORY STICKS – POTENTIAL THREAT
- HARDWARE RECYCLING
- ACCESS TO DATA
- BYOD – SMARTPHONES, ENCRYPTION.

PENALTIES

THE NEW DATA PROTECTION ACT 2018 WILL INCLUDE:

" A CRIMINAL OFFENCE OF 'KNOWING OR RECKLESSLY' OBTAINING OR DISCLOSING PERSONAL DATA WITHOUT THE CONSENT TO THE DATA CONTROLLER. THIS CAN INCLUDE HUMAN ERROR SUCH AS LOSING A MEMORY STICK WITH DATA ON IT, LEAVING FILES OUT ON PUBLIC VIEW OR SENDING AN EMAIL WITH DATA TO THE WRONG ADDRESS…OR AN OVERHEARD CONVERSATION."

THERE IS A 'RISK OF PERSONAL LIABILITY' IN WHICH COMPENSATION CAN BE SOUGHT IN ADDITION TO A FINE ISSUED BY THE INFORMATION COMMISSIONER'S OFFICE (ICO)

PENALTIES

- ICO HAS THE POWER TO ISSUE FINES OF UP TO 20 MILLION EUROS.
- NEW CIVIL COMPENSATION POWERS.
- EXTENDED CRIMINAL PENALTIES.
- INVESTIGATION AND ASSESSMENT POWERS ARE EXTENDED.
- PERSONAL LIABILITY IS REINFORCED.

ACTIONS – CURRENT PROCEDURES

- ALWAYS KEEP PERSONAL DATA LOCKED AWAY WHEN NOT IN USE.
- ELECTRONIC DATA MUST ONLY BE ACCESSED & PROCESSED USING ENCRYPTED DEVICES.
- FOLLOW ALL GUIDANCE ON THE USE OF EMAILS – USE OF 'INTERNAL' IN SUBJECT, NO FORWARDING OF OTHERS' ADDRESSES.
- COMPUTERS SHOULD BE ALWAYS LOCKED WHEN NOT ATTENDED.
- DATA TAKEN AWAY FROM THE SITE MUST BE STORED SAFELY.
- NEVER SHARE INFORMATION UNLESS THERE IS SPECIFIC PERMISSION OR IN NOT DOING, WOULD SERIOUSLY AFFECT THE WELFARE OF A CHILD.
- NEVER STORE OTHERS' PERSONAL DATA ON PERSONAL EQUIPMENT.

ACTIONS - NEW

- REMOVAL OF ALL MEMORY STICKS.
- REMOVAL OF 'OFF-LINE FILES' CAPACITY.
- IDENTIFY AND REMOVE ANY DATA THAT IS 'OUT OF DATE'.
- CHECK ENCRYPTION AND SECURITY OF OWN DEVICES.

- ASK YOURSELF, WOULD YOU BE HAPPY IF IT WAS YOUR OR YOUR FAMILY'S PERSONAL DATA BEING HANDLED IN THIS WAY?

COMPLIANCE IS MANDATORY